********** UNCLASSIFIED // **********

Subject: INTERNET-BASED CAPABILITIES GUIDANCE - UNOFFICIAL INTERNET POSTS
Originator: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=SECNAV WASHINGTON DC(UC)
DTG: 192031Z Aug 10
Precedence: ROUTINE
DAC: General
To: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ADDRESS LISTS(UC)/CN=AL ALNAV(UC)
    /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=AIG 6-AZ/OU=ALNAV
cc: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=CNO WASHINGTON DC(UC)
    /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=SECNAV WASHINGTON DC(UC)

UNCLASSIFIED//
FM SECNAV WASHINGTON DC
TO ALNAV
BT UNCLAS //N05230//
ALNAV 057/10

MSGID/GENADMIN/SECNAV WASHINGTON DC/AUG//

SUBJ/INTERNET-BASED CAPABILITIES GUIDANCE - UNOFFICIAL INTERNET POSTS//

REF/A/DESC: DIRECTIVE-TYPE MEMORANDUM (DTM) 09-26/DEPSECDEF/25FEB2010//
REF/B/DESC: DOD REGULATION 5500.7R/GC, DOD/23MAR2006//
REF/C/DESC: SECNAVINST 5211.5E/DNS-36/28DEC2005//
REF/D/DESC: SECNAVINST 5720.44B/OI-5/1NOV2005//

NARR/REF A IS DOD POLICY FOR THE RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES. REF B IS THE DOD JOINT ETHICS REGULATION. REF C IS THE DON PRIVACY PROGRAM. REF D IS THE DON PUBLIC AFFAIRS POLICY AND REGULATIONS.//

POC/ANN ANDREW/CIV/DON CIO/TEL: 703-607-5608/EMAIL: ANN.ANDREW(AT)NAVY.MIL// POC/ALAN GOLDSTEIN/CIV/CHINFO/TEL: 703-695-1887/EMAIL: ALAN.P.GOLDSTEIN(AT)NAVY.MIL// POC/RAY LETTEER/CIV/HQMC(C4)/TEL:703-693-3490-X128/EMAIL:RAY.LETTEER(AT)USMC.MIL//
POC/JULIANA ROSATI/CDR/OPNAVN2N6C3/TEL: 703-601-1717/EMAIL: JULIANA.ROSATI(AT)NAVY.MIL//

GENTEXT/REMARKS/1. THIS ALNAV PROVIDES GUIDANCE TO ALL DEPARTMENT OF NAVY (DON) PERSONNEL REGARDING UNOFFICIAL POSTS ON THE INTERNET, INCLUDING THOSE PERTAINING TO DON-RELATED CONTENT AND DISCUSSIONS. IT ALSO PROVIDES GUIDANCE ABOUT BEST-PRACTICES FOR USE OF INTERNET-BASED CAPABILITIES (IBC) IN A PERSONAL CAPACITY. A SEPARATE ALNAV PROVIDES GUIDANCE FOR EXTERNAL OFFICIAL PRESENCES ON IBC ON BEHALF OF THE DON.

A. "DON PERSONNEL" IS DEFINED AS ACTIVE-DUTY AND RESERVE COMPONENT SAILORS AND MARINES AND CIVILIAN EMPLOYEES OF THE DON.

B. PER REF A, IBC ARE DEFINED AS PUBLICLY ACCESSIBLE INFORMATION CAPABILITIES AND APPLICATIONS AVAILABLE ACROSS THE INTERNET IN LOCATIONS NOT OWNED, OPERATED, OR CONTROLLED BY THE DEPARTMENT OF DEFENSE OR THE FEDERAL GOVERNMENT. IBC INCLUDES COLLABORATIVE TOOLS SUCH AS SOCIAL NETWORKING SERVICES, SOCIAL MEDIA, USER-GENERATED CONTENT, SOCIAL SOFTWARE, WEB-BASED E-MAIL, INSTANT MESSAGING, AND DISCUSSION FORUMS (E.G., YOUTUBE, FACEBOOK, MYSPACE, TWITTER, GOOGLE APPS).

C. OFFICIAL INTERNET POSTS INVOLVE CONTENT THAT HAS BEEN RELEASED IN AN OFFICIAL CAPACITY BY DON PUBLIC AFFAIRS PERSONNEL OR COMMANDERS DESIGNATED AS RELEASING AUTHORITIES.

D. "UNOFFICIAL INTERNET POSTS" IS DEFINED AS ANY CONTENT ABOUT THE DON OR RELATED TO THE DON THAT IS POSTED ON ANY INTERNET SITE BY DON PERSONNEL IN AN UNOFFICIAL AND PERSONAL CAPACITY. CONTENT INCLUDES, BUT IS NOT LIMITED TO, PERSONAL COMMENTS, PHOTOGRAPHS, VIDEO, AND GRAPHICS. INTERNET SITES INCLUDE SOCIAL NETWORKING SITES, BLOGS, FORUMS, PHOTO- AND VIDEO-SHARING SITES, AND OTHER SITES, TO INCLUDE SITES NOT OWNED, OPERATED OR CONTROLLED BY THE DON OR DEPARTMENT OF DEFENSE. UNOFFICIAL INTERNET POSTS ARE NOT ENDORSED BY ANY PART OF THE DON OR REVIEWED WITHIN ANY OFFICIAL DON APPROVAL PROCESS.

2. PER THE GUIDELINES PROVIDED IN THIS ALNAV, DON PERSONNEL ARE ENCOURAGED TO RESPONSIBLY ENGAGE IN UNOFFICIAL INTERNET POSTING ABOUT THE DON AND DON-RELATED TOPICS. THE NAVY AND MARINE CORPS PERFORM A VALUABLE SERVICE AROUND THE WORLD EVERY DAY AND DON PERSONNEL ARE FREQUENTLY IN A POSITION TO SHARE OUR SUCCESSES WITH A GLOBAL AUDIENCE VIA THE INTERNET.

3. GUIDELINES. DON PERSONNEL ARE RESPONSIBLE FOR ALL DON-RELATED CONTENT THEY PUBLISH ON SOCIAL NETWORKING SITES, BLOGS, OR OTHER IBC AND SHOULD ENSURE THAT THIS CONTENT IS ACCURATE, APPROPRIATE AND DOES NOT COMPROMISE MISSION SECURITY OR SUCCESS. IN ADDITION TO ENSURING DON-RELATED CONTENT IS ACCURATE AND APPROPRIATE, IT IS RECOMMENDED THAT DON PERSONNEL BE MINDFUL ABOUT THE NON-DEPARTMENT RELATED CONTENT THEY POST SINCE THE LINES BETWEEN PERSONAL AND PROFESSIONAL LIVES OFTEN BLUR IN THE ONLINE SPACE. ALSO, DON PERSONNEL MUST BE AWARE THAT ONCE THEY POST CONTENT TO THE INTERNET, THEY LOSE CONTROL OF IT; MANY SOCIAL MEDIA SITES HAVE POLICIES THAT GIVE THEM OWNERSHIP OF ALL CONTENT AND INFORMATION POSTED OR STORED ON THEIR SYSTEMS. THUS DON PERSONNEL SHOULD USE THEIR BEST JUDGMENT AT ALL TIMES AND KEEP IN MIND HOW THE CONTENT OF THEIR POSTS WILL REFLECT UPON THEMSELVES, THEIR SERVICE, AND THE DON. THE FOLLOWING GUIDELINES ARE ESTABLISHED TO ASSIST WITH THIS RESPONSIBILITY:

A. DON PERSONNEL ENGAGED IN UNOFFICIAL INTERNET POSTING ABOUT THE DON MAY IDENTIFY THEMSELVES AS DON PERSONNEL BY RANK, BILLET, MILITARY OCCUPATIONAL SPECIALTY, AND STATUS (ACTIVE, RESERVE, CIVILIAN, ETC.) IF DESIRED. HOWEVER, IF DON PERSONNEL DECIDE TO IDENTIFY THEMSELVES AS DON PERSONNEL, THEY MUST NOT DISGUISE, IMPERSONATE OR OTHERWISE MISREPRESENT THEIR IDENTITY OR AFFILIATION WITH THE DON. WHEN EXPRESSING DON-RELATED PERSONAL OPINIONS, DON PERSONNEL SHOULD MAKE CLEAR THAT THEY ARE SPEAKING FOR THEMSELVES AND NOT ON BEHALF OF THE DON.

B. USE OF PERSONAL EMAIL ADDRESSES IS STRONGLY ENCOURAGED WHEN ENGAGING IBC FOR UNOFFICIAL PURPOSES. THIS INCLUDES, BUT IS NOT LIMITED TO, REGISTRATION WITH SOCIAL NETWORKING SITES AND COMMENTING IN FORUMS AND BLOGS. WHEN IT IS NOT FEASIBLE TO MAKE USE OF PERSONAL EMAIL ADDRESSES FOR THESE PURPOSES, DON PERSONNEL MAY USE THEIR DON PROVIDED EMAIL ADDRESSES.

C. AS WITH OTHER FORMS OF COMMUNICATION, DON PERSONNEL ARE RESPONSIBLE FOR ADHERING TO DON REGULATIONS AND POLICIES WHEN MAKING UNOFFICIAL INTERNET POSTS. DON PERSONNEL SHOULD COMPLY WITH REGULATIONS AND POLICIES SUCH AS PERSONAL STANDARDS OF CONDUCT, OPERATIONS SECURITY, INFORMATION ASSURANCE, PERSONALLY IDENTIFIABLE INFORMATION (PII), JOINT ETHICS REGULATIONS, AND THE RELEASE OF INFORMATION TO THE PUBLIC. VIOLATIONS OF REGULATIONS OR POLICIES MAY RESULT IN DISCIPLINARY ACTION. SEE REFS B AND C.

D. THE POSTING OR DISCLOSURE OF INTERNAL DON DOCUMENTS OR INFORMATION THAT THE DON HAS NOT OFFICIALLY RELEASED TO THE PUBLIC IS PROHIBITED. THIS INCLUDES CLASSIFIED, CONTROLLED UNCLASSIFIED INFORMATION (CUI), OR SENSITIVE INFORMATION (FOR EXAMPLE, TACTICS, TROOP MOVEMENTS, FORCE SIZE, WEAPON SYSTEM DETAILS, ETC). THIS POLICY APPLIES NO MATTER HOW DON PERSONNEL COME INTO POSSESSION OF THE INFORMATION OR DOCUMENT. EXAMPLES INCLUDE, BUT ARE NOT LIMITED TO, MEMOS, E-MAILS, MEETING NOTES, MESSAGE TRAFFIC, WHITE PAPERS, PUBLIC AFFAIRS GUIDANCE, PRE-DECISIONAL MATERIALS, INVESTIGATORY INFORMATION, AND PROPRIETARY INFORMATION. DON PERSONNEL ARE ALSO PROHIBITED FROM RELEASING OTHER THAN THEIR OWN DON E-MAIL ADDRESSES, TELEPHONE NUMBERS, OR FAX NUMBERS NOT ALREADY AUTHORIZED FOR PUBLIC RELEASE. WHEN IN DOUBT, DON PERSONNEL SHOULD CONTACT THEIR OPERATIONS SECURITY OFFICER, INTELLIGENCE OFFICER, FREEDOM OF INFORMATION ACT (FOIA) OFFICIAL, OR PUBLIC AFFAIRS OFFICER FOR GUIDANCE.

E. WHEN CORRECTING ERRORS AND MISREPRESENTATIONS MADE ABOUT THE DON, PERSONNEL ARE ENCOURAGED TO BE PROFESSIONAL AND RESPECTFUL. DON PERSONNEL SHOULD REFER TO THE CHAIN OF COMMAND OR PUBLIC AFFAIRS FOR GUIDANCE IF UNCERTAIN ABOUT THE NEED FOR, OR APPROPRIATENESS OF, A RESPONSE.

F. DON PERSONNEL SHOULD BE AWARE THAT THE INTERNET IS OFTEN USED TO GAIN INFORMATION FOR CRIMINAL ACTIVITIES SUCH AS IDENTITY THEFT. BY PIECING TOGETHER INFORMATION PROVIDED ON DIFFERENT WEBSITES, CRIMINALS CAN USE INFORMATION TO, AMONG OTHER THINGS, IMPERSONATE DON PERSONNEL, STEAL PASSWORDS, AND COMPROMISE DON NETWORKS. THEREFORE, WHEN USING THE INTERNET AND SOCIAL MEDIA, DON PERSONNEL SHOULD BE CAUTIOUS AND GUARD AGAINST CYBER CRIMINALS AND ATTACKERS BY ADHERING TO THE FOLLOWING SECURITY PROCEDURES.

(1) DON PERSONNEL SHOULD BE MINDFUL OF RELEASING PII THAT COULD BE USED TO DISTINGUISH THEIR INDIVIDUAL IDENTITY OR THAT OF ANOTHER INDIVIDUAL. EXAMPLES OF PII INCLUDE SOCIAL SECURITY NUMBER, ADDRESS, BIRTHDAY, BIRTH PLACE, DRIVER'S LICENSE NUMBER, ETC.

(2) DON PERSONNEL SHOULD BE CAREFUL WHEN RESPONDING VIA EMAIL TO IBC AUTOMATIC NOTIFICATIONS, SINCE THIS MAY INADVERTENTLY EXPOSE PERSONAL AND WORK RELATED CONTACT INFORMATION CONTAINED IN THE EMAIL SIGNATURE LINE.

(3) DON PERSONNEL SHOULD NOT CLICK LINKS OR OPEN ATTACHMENTS UNLESS THEY TRUST THE SOURCE. CYBER CRIMINALS OFTEN PRETEND TO BE PEOPLE THEY ARE NOT IN ORDER TO DECEIVE INDIVIDUALS INTO PERFORMING ACTIONS THAT LAUNCH CYBER ATTACKS, DOWNLOAD VIRUSES, AND INSTALL MALWARE AND SPYWARE ONTO COMPUTERS. TO HELP MITIGATE THESE THREATS, DON PERSONNEL SHOULD INSTALL AND MAINTAIN CURRENT ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE ON THEIR PERSONAL COMPUTERS. MILITARY AND CIVILIAN EMPLOYEES OF THE DON MAY OBTAIN ANTI-VIRUS SOFTWARE FOR HOME USE, FROM HTTPS://INFOSEC.NAVY.MIL/AV OR HTTPS://WWW.JTFGNO.MIL/ANTIVIRUS/ANTIVIRUS_HOMEUSE.HTM. YOU MUST ACCESS THESE SITES FROM A .MIL DOMAIN.

(4) DON PERSONNEL SHOULD ALWAYS USE THE STRONGEST PASSWORD COMBINATIONS ALLOWED, COMPRISED OF AS MANY OF THE COMBINATIONS OF LOWER- AND UPPER-CASE LETTERS, NUMBERS, AND SYMBOLS POSSIBLE. CHANGE PASSWORDS FREQUENTLY. USE DIFFERENT PASSWORDS FOR BANKING AND FINANCIAL SITES AND PERSONAL WEB-BASED EMAIL THAN THOSE FOR ANY OTHER SITE.

(5) DON PERSONNEL SHOULD BE THOUGHTFUL ABOUT WHO THEY ALLOW TO ACCESS THEIR SOCIAL MEDIA PROFILES (E.G. "FRIENDS" OR "FOLLOWERS" ON SITES SUCH AS FACEBOOK, MYSPACE, OR TWITTER) AND THUS ALLOW ACCESS TO THEIR PERSONAL INFORMATION. DON PERSONNEL SHOULD ALSO RECOGNIZE THAT SOCIAL NETWORK "FRIENDS" AND "FOLLOWERS" MAY POTENTIALLY CONSTITUTE RELATIONSHIPS THAT COULD AFFECT DETERMINATIONS IN BACKGROUND INVESTIGATIONS AND PERIODIC REINVESTIGATIONS ASSOCIATED WITH SECURITY CLEARANCES.

(6) DON PERSONNEL SHOULD BE CAREFUL ABOUT USE OF THIRD PARTY APPLICATIONS ASSOCIATED WITH SOCIAL NETWORKING SITES, SINCE SUCH APPLICATIONS OFTEN HAVE ACCESS TO A USER'S PERSONAL INFORMATION.

(7) DON PERSONNEL ARE ENCOURAGED TO LEARN ABOUT AND USE THE PRIVACY SETTINGS ON SOCIAL MEDIA SITES, IN ORDER TO LIMIT THE INFORMATION THAT MIGHT BE UNINTENTIONALLY SHARED WITH "FRIENDS" AND THE BROADER SOCIAL NETWORKING COMMUNITY.

(8) DON PERSONNEL SHOULD REVIEW THEIR ACCOUNTS ON A REGULAR BASIS FOR POSSIBLE USE OR CHANGES BY UNAUTHORIZED USERS.

(9) DON PERSONNEL SHOULD REVIEW OTHER RESOURCES FOR SAFE USE OF SOCIAL NETWORKING SITES, AVAILABLE FROM HTTP://WWW.IOSS.GOV/SNS_SAFETY_CHECK.PDF, AND ARE REQUIRED TO TAKE MANDATORY ANNUAL INFORMATION ASSURANCE (IA) TRAINING, WHICH PROVIDES ADDITIONAL GUIDANCE, DIRECTION, AND BEST-PRACTICES ASSOCIATED WITH THE USE OF IBC.

4. THERE IS VALUE TO THE ACCESS AND USE OF IBC. FOLLOWING THE ABOVE GUIDELINES WILL HELP PREVENT THE COMPROMISE OF THE SAFETY AND SECURITY OF MISSIONS, PERSONNEL, AND NETWORKS.

5. RELEASED BY RAY MABUS, SECRETARY OF THE NAVY.// BT