

\*\*\*\*\* UNCLASSIFIED / \*\*\*\*\*

Subject: Acceptable Use Policy for Department of the Navy (DON) Information Technology (IT) Resources  
Originator: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=DON CIO WASHINGTON DC(UC)

DTG: 031648Z Oct 11

Precedence: ROUTINE

DAC: General

To: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=AAUSN OPTI WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=ASSTSECNAV FM WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=ASSTSECNAV IE WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=ASSTSECNAV MRA WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=ASSTSECNAV RDA WASHINGTON DC(UC)

/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=USMC/OU=ORGANIZATIONS/L=HQMC WASHINGTON DC/OU=CMC WASHINGTON DC(UC)/OU=CMC WASHINGTON DC C4(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=USMC/OU=ORGANIZATIONS/L=HQMC WASHINGTON DC/OU=CMC WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=OGC WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=OLA WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=N/OU=NAVY JAG WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=CHINFO WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF COLUMBIA/L=WASHINGTON/OU=NAVINSGEN WASHINGTON DC(UC)

cc: /C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMPACFLT PEARL HARBOR HI

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=O-Q/OU=ONI WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=RHODE ISLAND/L=NEWPORT/OU=NAVWARCOL NEWPORT RI(UC)

/C=US/O=U.S.

GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=MARYLAND/L=ANNAPOLIS/OU=USNA ANNAPOLIS MD(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMFLTCYBERCOM FT GEORGE G MEADE MD

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVAIRSYSCOM PATUXENT RIVER MD

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVSUPSYSCOM MECHANICSBURG PA

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMSPAWARSSYSCOM  
SAN DIEGO CA

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVFACENCOM  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVSAFECEN  
NORFOLK VA

/C=US/O=U.S.  
GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(MC)/L=CALIFORNIA/L=CORONADO/OU=COM  
NAVSPECWARCOM CORONADO CA(MC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=N/OU=NETC PENSACOLA FL

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMUSNAVSO

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF  
COLUMBIA/L=WASHINGTON/OU=CNIC WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF  
COLUMBIA/L=WASHINGTON/OU=BUMED WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=N/OU=NAVAUDSVC WASHINGTON  
DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=D/OU=DIRNAVCRIMINVSERV  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(MC)/L=DISTRICT OF  
COLUMBIA/L=WASHINGTON/OU=DIRSSP WASHINGTON DC(MC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMUSNAVEUR NAPLES  
IT

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CT-CZ/OU=CUSFFC N6 NORFOLK VA

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=USMC/OU=ORGANIZATIONS/L=MCB QUANTICO  
VA/OU=COMMARCORSYSCOM/OU=COMMARCORSYSCOM QUANTICO VA(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVSEASYSYSCOM  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVRESFORCOM  
NORFOLK VA

/C=US/O=U.S.  
GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(MC)/OU=MOBILES/OU=COMUSNAVCENT(MC  
)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=NAVY/OU=ORGANIZATIONS(UC)/L=DISTRICT OF  
COLUMBIA/L=WASHINGTON/OU=CHNAVPER WASHINGTON DC(UC)

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAVLEGSVCCOM  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=N/OU=NAVHISTHERITAGECOM  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAV CYBERFOR  
VIRGINIA BEACH VA

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=CE-CS/OU=COMNAV DIST  
WASHINGTON DC

/C=US/O=U.S. GOVERNMENT/OU=DOD/OU=AUTODIN PLAS/OU=N/OU=NAVY BAND WASHINGTON  
DC

-----  
UNCLASSIFIED/  
UNCLAS

MSGID/GENADMIN/DON CIO WASHINGTON DC//

SUBJ/ACCEPTABLE USE POLICY FOR DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT) RESOURCES//

REF/A/MSG/DON CIO/161108ZJUL05//

REF/B/DOC/DOD/23MAR2006//

REF/C/DOC/DOD/25FEB2010//

REF/D/DOC/DOD/06FEB2003//

REF/E/DOC/DON/01JUN2006//

REF/F/MSG/SECNAV/192027ZAUG10//

REF/G/MSG/SECNAV/192031ZAUG10//

REF/H/DOC/DON CIO/17JUN2009//

REF/I/DOC/SECNAV/31DEC2005

REF/J/MSG/DON CIO/032009ZOCT08//

NARR/REF A IS DON CIO MESSAGE ON EFFECTIVE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY RESOURCES. REF B IS DEPARTMENT OF DEFENSE (DOD) 5500.7R, JOINT ETHICS REGULATION, SEC 2-301. REF C IS DEPSECDEF DIRECTIVE-TYPE MEMORANDUM 09-026 ON RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES. REF D IS DODI 8500.2, INFORMATION ASSURANCE (IA) IMPLEMENTATION. REF E IS SECNAV M-5510.30, DON PERSONNEL SECURITY PROGRAM. REF F IS ALNAV 056/10 THAT PROVIDES SECNAV GUIDANCE FOR OFFICIAL POSTS ON INTERNET-BASED CAPABILITIES. REF G IS ALNAV 057/10 THAT PROVIDES SECNAV GUIDANCE FOR UNOFFICIAL POSTS ON INTERNET-BASED CAPABILITIES. REF H IS SECNAVINST 5239.3B, DEPARTMENT OF THE NAVY INFORMATION ASSURANCE (IA) POLICY. REF I IS THE DON NAVY RECORDS MANAGEMENT PROGRAM. REF J PROVIDES SECNAV POLICY ON THE USE OF DIGITAL SIGNATURES AND ENCRYPTION WITH EMAIL.//

POC/DAN DELGROSSO/GS15/DON CIO/LOC: ARLINGTON VA/TEL: 703-695-2900/  
EMAIL:DAN.DELGROSSO(AT)NAVY.MIL //

POC/RAY LETTEER/GS15/HQMC C4/LOC: ARLINGTON VA/TEL: 703-693-3490/  
EMAIL: RAY.LETTEER(AT)USMC.MIL//

POC/JULIANA ROSATI/CDR/OPNAV N2N6/LOC: ARLINGTON VA/TEL: 571-256-8523/ EMAIL:  
JULIANA.ROSATI(AT)NAVY.MIL//

PASSING INSTRUCTIONS:

CNO: PLEASE PASS TO DNS/N091/N093/N095/N097/N1/N2N6/N3/N5/N4/N8//

CMC: PLEASE PASS TO DCMS/ACMC/AR/M&RA/I/I&L/PP&O/C4/P&R/MAJCOMS

RMKS/1. PURPOSE. CANCEL REF A. IN SUPPORT OF REFS B AND C, THIS MESSAGE OUTLINES ACCEPTABLE USE STANDARDS WHEN USING DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT) RESOURCES FOR OFFICIAL AND AUTHORIZED UNOFFICIAL PURPOSES.

2. SCOPE AND APPLICABILITY. THIS MESSAGE APPLIES TO ALL DON INFORMATION TECHNOLOGY (IT) RESOURCE USERS TO INCLUDE MILITARY, CIVILIAN AND CONTRACT SUPPORT PERSONNEL.

3. BACKGROUND. WHEN USED APPROPRIATELY, DON IT RESOURCES GREATLY ENHANCE OUR WARFIGHTING AND BUSINESS PROCESSING CAPABILITIES. HOWEVER, WHEN USED INAPPROPRIATELY AND WITHOUT REGARD TO GOOD PRACTICES, THESE SAME RESOURCES INCREASE THE DON'S EXPOSURE TO MALICIOUS INTRUSIONS, EXPOSE OUR INFORMATION TO THREATS, AND INCREASE COSTS THROUGH SPILLAGE AND HIGHER BANDWIDTH (B/W) REQUIREMENTS. ADDITIONALLY, THE COMBINED EFFECT OF RECREATIONAL INTERNET SURFING AND NON-MISSION RELATED HIGH B/W INTENSIVE ACTIVITIES (E.G., STREAMING MEDIA SUCH AS MOVIES OR MUSIC VIDEOS, DOWNLOADING IMAGES FOR PERSONAL USE, ETC.), IMPACTS OVERALL NETWORK PERFORMANCE AND MAY IMPEDE CRITICAL BUSINESS AND MISSION NEEDS. RECENT METRICS FROM THE DEFENSE INFORMATION SYSTEMS AGENCY SHOW THAT OF THE TOP 50 WEBSITES VISITED BY DON USERS, NEARLY 48 PERCENT OF THEM ARE HIGH INTENSIVE B/W WEBSITES OR LIKELY NON-MISSION SITES OR BOTH. THIS FIGURE EXCEEDS THE DEPARTMENT OF DEFENSE (DOD)-WIDE AVERAGE BY 6 PERCENT.

#### 4. DISCUSSION:

A. APPROPRIATELY CONTROLLING ACCESS TO, AND PERSONAL USE OF, DON IT RESOURCES IS A LEADERSHIP ISSUE. COMMANDERS, COMMANDING OFFICERS, CIVILIAN LEADERS AND OFFICERS IN CHARGE MUST ENGAGE WITH THEIR USERS TO ENSURE IT RESOURCES ARE BEING UTILIZED IN AN ACCEPTABLE MANNER AND IN ACCORDANCE WITH THE BELOW POLICY. FOLLOWING THIS POLICY AND INSTILLING A CLIMATE OF ACCOUNTABILITY COMBINED WITH AN EFFECTIVE COMMAND TRAINING PROGRAM (TO INCLUDE DOD INFORMATION ASSURANCE (IA) AWARENESS TRAINING) AND SIGNED SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR) FORM), WILL ENHANCE PRODUCTIVITY, MAINTAIN NETWORK STABILITY, AND SUPPORT A SOLID DEFENSE-IN-DEPTH APPROACH.

B. AS STATED IN REF C, COMMANDERS AT ALL LEVELS SHALL CONTINUE TO DEFEND AGAINST MALICIOUS ACTIVITY AFFECTING DON NETWORKS (E.G., DISTRIBUTED DENIAL OF SERVICE ATTACKS, INTRUSIONS, ETC.) AND TAKE IMMEDIATE AND COMMENSURATE ACTIONS, AS REQUIRED, TO SAFEGUARD MISSIONS (E.G., TEMPORARILY LIMITING ACCESS TO THE INTERNET TO PRESERVE OPERATIONS SECURITY OR TO ADDRESS B/W CONSTRAINTS). CIRCUMSTANCES REQUIRING LONG TERM ACTION (E.G., EXTENSIVE ACCESS DENIAL TO COMMERCIAL EMAIL OR HIGH BANDWIDTH INTENSIVE WEBSITES) REQUIRE COORDINATION WITH THE DON CHIEF INFORMATION OFFICER (CIO).

C. USERS ARE REMINDED THAT EXISTING MONITORING TOOLS ARE IN PLACE TO OBSERVE USER ACTIVITY AND TO IMPLEMENT VARYING LEVELS OF FILTERING RESTRICTIONS, SHOULD THE NETWORK BEGIN TO REACH MAXIMUM B/W OPERATING CAPACITY. UNDER DOD, DON, AND SERVICE DIRECTIVES, COMMUNICATIONS USING, OR DATA STORED ON, DOD INFORMATION SYSTEMS ARE NOT PRIVATE; ARE SUBJECT TO ROUTINE MONITORING, INTERCEPTION, AND SEARCH; AND MAY BE DISCLOSED FOR ANY AUTHORIZED GOVERNMENT PURPOSES.

#### 5. POLICY

A. COMMANDS SHALL ENSURE REQUIRED BACKGROUND INVESTIGATIONS ARE COMPLETED COMMENSURATE WITH THE LEVEL OF NETWORK ACCESS REQUIRED, PER REFS D AND E. ALL USERS SHALL HAVE AN APPROVED SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR) FORM ON FILE PRIOR TO BEING GRANTED ACCESS TO DON NETWORKS.

B. ALL USERS SHALL COMPLETE DOD IA AWARENESS TRAINING PRIOR TO BEING GRANTED ACCESS TO DOD INFORMATION SYSTEMS AND ANNUALLY THEREAFTER AS A CONDITION OF CONTINUED ACCESS TO THE SYSTEM.

C. ALL USERS SHALL COMPLETE PERSONALLY IDENTIFIABLE INFORMATION (PII) TRAINING ANNUALLY.

D. DON IT RESOURCES ARE PROVIDED FOR OFFICIAL USE AND AUTHORIZED PURPOSES ONLY. AUTHORIZED PURPOSES MAY INCLUDE PERSONAL USE WITHIN THE LIMITATIONS SET FORTH IN REF B. PERSONAL USE MUST NOT ADVERSELY AFFECT THE PERFORMANCE OF OFFICIAL DUTIES, DEGRADE NETWORK PERFORMANCE, AND MUST BE OF A REASONABLE DURATION AND FREQUENCY AS DETERMINED BY COMMANDING OFFICERS AND SUPERVISORS. THIS INCLUDES PERSONAL COMMUNICATIONS FROM THE DON EMPLOYEE'S USUAL WORK PLACE THAT ARE MOST REASONABLY MADE DURING THE WORK DAY (SUCH AS CHECKING IN WITH SPOUSE OR MINOR CHILDREN; SCHEDULING DOCTOR AND AUTO OR HOME REPAIR APPOINTMENTS; BRIEF INTERNET SEARCHES; E-MAILING DIRECTIONS TO VISITING RELATIVES, CONDUCTING ON-LINE BANKING, DISTANCE LEARNING, ETC.). FOR NON-EMERGENCY SITUATIONS, PERSONAL COMMUNICATIONS SHALL BE MADE DURING THE DON EMPLOYEE'S PERSONAL TIME SUCH AS AFTER DUTY HOURS OR LUNCH PERIODS.

E. COMMERCIAL EMAIL.

(1) DON PERSONNEL ARE AUTHORIZED TO ACCESS COMMERCIAL WEB-BASED EMAIL USING DON IT RESOURCES FOR PERSONAL USE WITHIN THE LIMITATIONS OF PARA 5.D.

(2) USE OF COMMERCIAL EMAIL FOR OFFICIAL BUSINESS IS ONLY PERMITTED WHEN NECESSARY TO MEET OPERATIONAL REQUIREMENTS IN CASES WHEN DON PROVIDED EMAIL IS UNAVAILABLE. THIS USE MUST BE ENDORSED BY THE FIRST O-6/GS-15 IN THE CHAIN OF COMMAND AND APPROVED IN ADVANCE BY THE DESIGNATED ACCREDITING AUTHORITY (DAA) RESPONSIBLE FOR THE SPECIFIC NETWORK (OR THE DAA'S WRITTEN DESIGNEE).

(3) USERS MUST FOLLOW SPECIFIC GUIDELINES DEFINED IN REFS F AND G TO ENSURE CONTROLLED UNCLASSIFIED INFORMATION (CUI), INCLUDING PII AND FOR OFFICIAL USE ONLY (FOUO) IS SAFEGUARDED. COMMERCIAL EMAIL CANNOT BE AUTHORIZED TO TRANSMIT UNENCRYPTED CUI, TO INCLUDE PII.

(4) ANY RECORDS GENERATED THROUGH USE OF COMMERCIAL EMAIL FOR OFFICIAL BUSINESS MUST BE PROTECTED IAW REF H AND MAINTAINED IAW REF I.

F. TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AND SECURITY OF DON IT RESOURCES AND INFORMATION, USERS SHALL NOT:

(1) AUTO-FORWARD ANY E-MAIL FROM A DON ACCOUNT TO A COMMERCIAL E-MAIL ACCOUNT (I.E., .COM, .EDU, ETC.).

(2) BYPASS, STRESS, OR TEST IA OR COMPUTER NETWORK DEFENSE (CND) MECHANISMS (E.G., FIREWALLS, CONTENT FILTERS, PROXY SERVERS, ANTI-VIRUS PROGRAMS).

(3) INTRODUCE OR USE UNAUTHORIZED SOFTWARE, FIRMWARE, OR HARDWARE ON ANY DON IT RESOURCE.

(4) RELOCATE OR CHANGE EQUIPMENT OR THE NETWORK CONNECTIVITY OF EQUIPMENT WITHOUT AUTHORIZATION FROM THE LOCAL IA AUTHORITY (I.E., PERSON RESPONSIBLE FOR THE OVERALL IMPLEMENTATION OF IA AT THE COMMAND LEVEL).

(5) USE PERSONALLY OWNED HARDWARE, SOFTWARE, SHAREWARE, OR PUBLIC DOMAIN SOFTWARE WITHOUT WRITTEN AUTHORIZATION FROM THE LOCAL IA AUTHORITY.

(6) UPLOAD/DOWNLOAD EXECUTABLE FILES (E.G., .EXE, .COM, .VBS, OR .BAT) ONTO DON IT RESOURCES WITHOUT THE WRITTEN APPROVAL OF THE LOCAL IA AUTHORITY.

(7) PARTICIPATE IN OR CONTRIBUTE TO ANY ACTIVITY RESULTING IN A DISRUPTION OR DENIAL OF SERVICE.

(8) WRITE, CODE, COMPILE, STORE, TRANSMIT, TRANSFER, OR INTRODUCE MALICIOUS SOFTWARE, PROGRAMS, OR CODE.

(9) IAW REF (B), USE DON IT RESOURCES IN A WAY THAT WOULD REFLECT ADVERSELY ON THE DON. SUCH USES INCLUDE PORNOGRAPHY, CHAIN LETTERS, UNOFFICIAL ADVERTISING, SOLICITING OR SELLING EXCEPT ON AUTHORIZED BULLETIN BOARDS ESTABLISHED FOR SUCH USE, VIOLATION OF STATUTE OR REGULATION, INAPPROPRIATELY HANDLED CLASSIFIED INFORMATION AND PII, AND OTHER USES THAT ARE INCOMPATIBLE WITH PUBLIC SERVICE.

(10) PLACE DATA ONTO DON IT RESOURCES POSSESSING INSUFFICIENT SECURITY CONTROLS TO PROTECT THAT DATA AT THE REQUIRED CLASSIFICATION (E.G., SECRET ONTO UNCLASSIFIED).

G. TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AND SECURITY OF DON IT RESOURCES AND INFORMATION, USERS SHALL:

(1) SAFEGUARD INFORMATION AND INFORMATION SYSTEMS FROM UNAUTHORIZED OR INADVERTENT MODIFICATION, DISCLOSURE, DESTRUCTION, OR MISUSE.

(2) PROTECT CUI, TO INCLUDE PII, AND CLASSIFIED INFORMATION TO PREVENT UNAUTHORIZED ACCESS, COMPROMISE, TAMPERING, OR EXPLOITATION OF THE INFORMATION.

(3) PROTECT AUTHENTICATORS (E.G., PASSWORDS AND PERSONAL IDENTIFICATION NUMBERS (PIN)) REQUIRED FOR LOGON AUTHENTICATION AT THE SAME CLASSIFICATION AS THE HIGHEST CLASSIFICATION OF THE INFORMATION ACCESSED.

(4) PROTECT AUTHENTICATION TOKENS (E.G., COMMON ACCESS CARD (CAC), ALTERNATE LOGON TOKEN (ALT), PERSONAL IDENTITY VERIFICATION (PIV), NATIONAL SECURITY SYSTEMS (NSS) TOKENS) AT ALL TIMES. AUTHENTICATION TOKENS SHALL NOT BE LEFT UNATTENDED AT ANY TIME UNLESS PROPERLY SECURED.

(5) VIRUS-CHECK ALL INFORMATION, PROGRAMS, AND OTHER FILES PRIOR TO UPLOADING ONTO ANY DON IT RESOURCE.

(6) REPORT ALL SECURITY INCIDENTS INCLUDING PII BREACHES IMMEDIATELY IN ACCORDANCE WITH APPLICABLE PROCEDURES.

(7) ACCESS ONLY THAT DATA, CONTROLLED INFORMATION, SOFTWARE, HARDWARE, AND FIRMWARE FOR WHICH THE USER IS AUTHORIZED ACCESS BY THE COGNIZANT DON COMMANDING OFFICER, HAS A NEED-TO-KNOW, AND HAS THE APPROPRIATE SECURITY CLEARANCE. ASSUME ONLY THOSE ROLES AND PRIVILEGES FOR WHICH THE USER IS AUTHORIZED.

(8) OBSERVE ALL POLICIES AND PROCEDURES GOVERNING THE SECURE OPERATION AND AUTHORIZED USE OF A DON INFORMATION SYSTEM.

(9) DIGITALLY SIGN AND ENCRYPT EMAIL IAW REF J.

(10) EMPLOY SOUND OPERATIONS SECURITY MEASURES IAW DOD, DON, SERVICE AND COMMAND DIRECTIVES.

6. ACTION. COMMAND LEADERSHIP SHALL FAMILIARIZE THEMSELVES WITH REFS B THROUGH J AND SHALL INCORPORATE APPLICABLE REQUIREMENTS AND GUIDELINES INTO COMMAND POLICY, GUIDANCE, TRAINING, AND ACCOUNTABILITY ACTIONS.

7. THIS MESSAGE REMAINS IN EFFECT UNTIL SUPERCEDED, UPDATED, OR CANCELLED.

8. REQUEST WIDEST DISSEMINATION. RELEASED BY TERRY A. HALVORSEN, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER. //