DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

12 February 2016

MEMORANDUM FOR DISTRIBUTION

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)

Ref: See Enclosure (1)

Encl: (1) References
(2) Acceptable Use of DON IT

This memorandum updates the Department of the Navy (DON) Acceptable Use Policy and cancels references (a) through (c). Enclosure (2) specifies acceptable use of DON IT. The DON uses tools to monitor user activity and to implement varying levels of capacity/filtering restrictions. Communications using, or information stored on, DON IT are not private and are subject to routine monitoring, interception, and search; and may be disclosed for any authorized government purposes.

This memorandum is a coordinated effort between the Deputy Under Secretary of the Navy for Policy (DUSN(P)) Security and the DON Chief Information Officer (DON CIO) as part of the DON's cyber/traditional security partnership for the protection of national security information and information systems.

DON IT resources greatly enhance our warfighting and business processing capabilities. 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 ensure users use DON IT resources in an acceptable manner and in accordance with policy. Adhering to this policy and instilling a climate of accountability combined with an effective command education program supports a solid defense-in-depth approach.

My point of contact for this policy is Darcee Branham, (757) 203-3741, darcee.branham@navy.mil.

Robert W. Foster

Distribution: (See Pages 2 & 3)

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)

Distribution:
ASN RD&A
ASN M&RA
ASN FM&C
ASN EI&E
GC
DON/AA
DUSN (M)
DUSN (P)
NAVIG
JAG
OLA
CHINFO
AUDGEN
CNR
DON CIO
SAPRO
NCIS
OPNAV N2/N6
HQMC C4
PEO EIS
PEO C4I
COMPACFLT
COMUSFLTFORCOM
COMUSNAVEUR USNAVAF
COMNAVAIRSYSCOM
COMNAVRESFORCOM
COMNAVSEASYSCOM
CNIC
COMUSNAVCENT
USNA
COMFLTCYBERCOM
BUMED
COMNAVSAFECEN
NETC
COMNAVLEGSVCCOM
COMNAVSUPSYSCOM
COMUSNAVSO
COMNAVFACENGCOM
NAVWARCOL
COMSPAWARSYSCOM
COMNAVSPECWARCOM
DIRSSP
BUPERS
COMNAVDIST

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY (DON) INFORMATION
TECHNOLOGY (IT)

Distribution: (continued)
ONI
NAVY BAND
FLDSUPPACT
NAVPGSCOL
NAVHISTHERITAGECOM

ENCLOSURE 1 – REFERENCES
February 10, 2016

(a) DON CIO MSG, "Acceptable Use Policy for DON IT Resources," DTG 031648Z Oct 11 (hereby canceled)
(b) DON CIO Memo Use of Alternate Tokens by GO/FO/SES and Their Designated Staff, of 6 May 2012 (hereby canceled)
(c) DON CIO MSG Remote access to Enterprise email from non-DOD users R 161957Z Oct 02 ZYB (hereby canceled)
(d) DoD 5500.7R, "Joint Ethics Regulation (JER), Change 7, Section 2-301," November 17, 2011
(e) DoDI 8500.01, "Cybersecurity," March 13, 2014
(f) SECNAV M-5510.30, "Department of the Navy Personnel Security Program," June 1, 2006
(g) SECNAV MSG, "Internet-Based Capabilities Guidance: Official Internet Posts," DTG 192027Z Aug 10
(h) SECNAV MSG, "Internet-Based Capabilities Guidance - Unofficial Internet Posts," DTG 192031Z Aug 10
(i) CNSSI 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended
(j) NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," current edition
(k) CJCSI 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," January 24, 2012
(l) DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(m) SECNAVINST 5510.30B, "DON Personnel Security Program (PSP) Instruction," October 6, 2006
(n) SECNAV M-5510.36, "Department of the Navy Information Security Program," June 2006
(o) SECNAVINST 5510.36A, "DON Information Security Program Instruction," October 6, 2006
(p) SECNAVINST 5510-34A, "Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives," October 8, 2004
(q) DoDD 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(r) DoDM 5200.01 (Vol 4), "DOD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
(s) DoDM 5200.01 (Vol 3), "DoD Information Security Program: Protection of Classified Information" February 24, 2012
(t) CJCS M-6510.01, "Cyber Incident Handling Program," July 10, 2012
(u) OMB M-06-16, "Protection of Sensitive Agency Information," June 23, 2006
(v) DoDD 5400.11, "DoD Privacy Program," October 29, 2014
(w) DoDI 1035.01, "Telework Policy," April 4, 2012
(x) SECDEF Memo "Security and Operational Guidance for Classified Portable Electronic Devices", August 19, 2015
(y) DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(z) SECNAVINST 5210.8E, "Department of the Navy Records Management Program," December 17, 2015

ENCLOSURE 2 – Acceptable Use of DON IT
February 10, 2016

1. General Use
   a. DON IT users are every Sailor, Marine, civilian, contract support person, or foreign national with approved access to DON IT.
   b. DON IT users must observe all policies and procedures governing the secure operation and authorized use of DON IT.
   c. Users of systems that impact financial statements will not only follow prescribed internal controls set by policies and procedures governing secure operation and authorized use of DON IT, they will also follow internal controls required per Federal Information System Control Audit Manual (FISCAM) audit methodology (available on the DON CIO web site: http://www.doncio.navy.mil).
   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 reference (d). Personal use must not adversely affect the performance of official duties or 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 IT users 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, emailing directions to visiting relatives, conducting on-line banking, distance learning, checking commercial email account, etc.). Non-emergency personal communications shall be made during personal time, such as after duty hours or lunch periods.
   e. Users must not use DON IT to access inappropriate web sites or applications. Any questions regarding appropriateness of web sites or applications should be addressed to supervisors.
   f. Users must not use DON IT in violation of the Hatch Act (5 U.S.C. §§ 7321-7326), which limits certain political activities of most federal executive branch civilian employees. Military personnel are similarly affected by Department of Defense Directive 1344.10, which mirrors the Hatch Act. The Hatch Act has a wide and evolving scope. Any questions regarding prohibited behaviors should be addressed to a supervisor or ethics officer. Below are some specific prohibitions; but not a comprehensive list. DON IT users must not:
      (1) Engage in political activity while on duty or in the workplace. This includes partisan political social media posts, "likes," shares, pictures, "tweets," "re-tweets," and sending email messages and links, etc., even when using an alias, personal social media account, or personal email account.
      (2) Send or forward partisan political communications via social media or email to a subordinate at any time.
      (3) Engage in political activity in an official capacity at any time, or refer to official titles or positions while engaged in political activities. This includes using an official email account or a social media account created for use in an official capacity to engage in political activity.
      (4) Suggest, solicit, or receive political contributions at any time. This includes sending or forwarding invitations to political fundraising events and providing links to partisan political contribution sites or pages.

(5) Forward partisan political emails received by a government account to anyone or any place other than their own personal email accounts.

g. DON IT users may not use official email addresses to sign up for non-official online services (e.g., adult content,)

h. Commands shall ensure required background investigations are completed commensurate with the level of DON IT access a user requires, per references (e) and (f).

i. All DON IT users shall have approved DON system authorization access requests (SAAR) on file prior to being granted access to DON networks.

j. DON IT users must not bypass, stress, or test cybersecurity (CS) or computer network defense (CND) mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs).

k. Users must not introduce or use unauthorized software, firmware, or hardware on any DON IT resource.

l. Users must not relocate or change equipment or the network connectivity of equipment without authorization from the local CS authority (i.e., person responsible for the overall implementation of CS at the command level, such as the Information System Security Manager).

m. Users must not use personally owned hardware, software, shareware, or public domain software for official DON business without written authorization from the local CS authority.

n. Users must not upload or download executable files (e.g., .exe, .com, .vbs, or .bat) onto DON IT resources without the written approval of the local CS authority.

o. Users must not use DON IT to participate in or contribute to any activity resulting in a disruption or denial of service.

p. Users must not use DON IT to write, develop, compile, store, transmit, transfer, or introduce unauthorized or malicious software, programs, or code.

q. In accordance with reference (d), users must not use DON IT resources in any way that would reflect poorly on the DON. Such uses include, but are not limited to, pornography, chain letters, unofficial advertising, soliciting or selling (except on authorized bulletin boards established for such use), violation of statute or regulation, inappropriate handling of classified information and Personally Identifiable Information (PII), and other uses that are incompatible with public service.

r. Users must follow the specific guidance provided in references (g) and (h) to properly safeguard controlled unclassified information (CUI), including PII and for official use only (FOUO).

s. Users must report all security incidents, including PII breaches, immediately in accordance with references (r), (s), (n) and Command policy and procedures.

t. Users must not place data onto DON IT resources whose security controls are insufficient to protect that data (i.e., data classified Secret may not be placed onto an unclassified network).

u. Users must protect DoD/DON Information and IT to prevent unauthorized access, compromise, tampering, exploitation, unauthorized or inadvertent modification, disclosure, destruction, or misuse

v. Users must 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.

w. Users must 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. Unattended tokens must be properly secured.
x. Users must virus-check all information, programs, and other files prior to uploading them onto any DON IT resource.
y. Users must access only that data, classified and unclassified controlled information, software, hardware, and firmware for which they are authorized access, have a need-to-know, and have the appropriate security clearance. Users must assume only those roles and privileges for which they are authorized.
z. Commanders of DON organizations shall obtain formal authorization to interconnect information systems and networks per references (e), (i), (j) and (k).
aa. DON organizations may use Internet based capabilities as defined in references (g), (h), (l) and other applicable policies.
bb. Commanders of DON organizations shall control the access of contractors and representatives of foreign nations, coalitions, or international organizations to DON IT and the information residing on those systems, in accordance with relevant national and DoD policies and guidance, including references (e), (f), (i), (j), (m), (n), (o), (p), and (q).

2. Training Requirements
   a. Users must complete DoD approved CS courses within 30 days after receiving access to DON IT. Commanders of DON organizations may add specific DON, Service, and local CS policies and procedures. DoD CS training includes initial orientation and an annual refresher course. Completing the annual CS refresher course is a condition that users must meet for continued use of DON IT.
   b. Users must complete personally identifiable information (PII) training annually.
   c. DON IT users must complete derivative classification training prior to being granted initial access to DON classified IT and biennially thereafter.

3. Email Use
   a. Users must digitally sign email messages requiring either message integrity or non-repudiation using DoD Public Key Infrastructure (PKI) or other approved method. All email containing an attachment or embedded active content must be digitally signed.
   b. Users must encrypt CUI contained in email in accordance with reference (r). Examples of this are attachments that contain personal identity or budget information.
   c. Use of commercial email for certain types of unclassified information for official government business is only permitted under the following conditions, and failure to comply may result in administrative or punitive action:
      (1) Pre-approval requirements:
         (a) To meet an urgent operational requirement(s) wherein the user will not have access to unclassified DON IT systems (e.g., NIPRNET). This method is not authorized as a routine means.
         (b) User must submit a request in writing and have it approved by a FO/GO/SES in the chain of command, prior to using commercial email. The request must include the urgent operational requirement(s) and validation of compliance with the requirements in subparagraph 2 and 3 below.

(c) FO/GO/SES personnel are considered sufficiently senior to pre-approve use of personal email when the conditions cited in 1.a above apply. However, they must still ensure compliance with the requirements in subparagraphs 2 and 3 below.

(d) A copy of the approval must be provided to DUSN(P) Security for reference.

(2) Records generated:

(a) Once approval has been obtained per requirements in paragraph 1 above, DON personnel must include their official government email address on all email transmissions containing DON unclassified information. Transmitting DON unclassified information to any other commercial email address is prohibited.

(b) If unable to copy their official government email address, users must forward complete copies of the information to their official government email address within 20 days of the original creation or transmission of the record per reference (z) and 44 U.S.C. § 2911.

(3) Level of information authorized and prohibited:

(a) Authorized (only when digitally signed and encrypted per DoD Manual 5200.01-Volume 4):

1. Unclassified official government information that does not require safeguarding and dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.

2. Unclassified//For Official Use Only (U//FOUO) information as defined in DoD Manual 5200.01-Volume 4, which is a type of controlled unclassified information (CUI). This includes FOUO information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended (i.e., Personally Identifiable Information (PII)).

(b) Prohibited:

1. Classified information.

2. All other current types of CUI outlined in DoD M-5200.01-Volume 4 and SECNAV M-5510.36, such as Department of State Sensitive But Unclassified, Drug Enforcement Administration Law Enforcement, Unclassified Naval Nuclear Propulsion Information, Unclassified Critical Nuclear Weapons Design Information, National Geospatial-Intelligence Agency unclassified imagery or geospatial information, unclassified Technical Documents with Distribution Statement F or X, etc.

d. Users must not auto-forward official email from their DON email accounts to commercial email accounts.

e. Commanders of DON organizations may authorize remote access via Outlook Web Access (OWA) to unclassified official email using personally owned and other non-DoD computers. Commanders and users must document the verifiable need, and ensure the approval; training, configuration, and process comply with DON and Service OWA policy.

(1) Users must:

(a) Submit a request/signed statement accepting responsibility for approved access for each computer expected to access email.

(b) Indicate a valid requirement (convenience alone is not a valid requirement)

(c) Use PKI authentication

(d) Handle, store, maintain and destroy all unclassified information in accordance with DoD and DON policies.
(e) Immediately notify their commands of any information loss, theft or suspicious behavior of their system(s).
(f) Protect the confidentiality, integrity and availability of DON e-mail systems and information at all times.
(g) Complete Service designed specific OWA training prior to accessing OWA.
(h) Install, configure, maintain and update required security software, hardware, PKI certificates and current anti-virus files by updating them at least weekly or when prompted.
(i) Not use public access computers, such as those in college computer labs, public kiosks, libraries, etc. to access DON or DoD unclassified e-mail accounts.
(j) Use Wireless Fidelity (WiFi) hotspots only if the connection and user complies with remote access requirements.
(k) Ensure that no other wireless or LAN connection exists for the duration of the OWA session. Any other existing connections must be disabled for the duration of the session.
(l) At the completion of an OWA session:
1. Close all DON email files;
2. Clear the web browser's cache;
3. Exit and close the browser; and
4. Immediately turn off the computer. "Sleep" and "standby" modes are not acceptable.

(2) Commanders of DON organizations must:
(a) Document authorization to use OWA by name or command wide with an authorized users list; maintain the authorized users list.
(b) Evaluate each request for validity and approve those essential for mission accomplishment.
(c) Retain all user signed statements until that member's detachment from the command.
(d) Review approvals annually.
(e) Disable access immediately upon a member's detachment.
(f) Conduct oversight for compliance and take appropriate actions for non-compliance.

4. Remote Access

a. Commanders of DON organizations shall control remote access to DON IT per references (e), (f), (i), (j), (m), (t), (u), and (v).
b. Commanders of DON organizations shall provide government-furnished computer equipment, software, and communications with appropriate security measures as the primary means for remote access for any regular and recurring telework arrangement that involves CUI information, per reference (w).
c. Commanders of DON organizations must ensure all remote access to DoD information systems and networks, including telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Use encryption to protect the confidentiality of the session, per reference (e).

d. Commanders of DON organizations must ensure authentication and confidentiality requirements for remote access sessions use National Security Agency (NSA)-approved COMSEC and keying material for classified systems and National Institute of Standards and Technology (NIST)-approved COMSEC and DoD PKI certificates for unclassified systems.

e. Commanders of DON organizations shall consider mandating the use of Virtual Private Networks (VPNs) to protect and control internal and external access to their information systems and networks, if a mission need for remote access is established. VPNs are the preferred method when using government-furnished or government-contracted equipment.

f. Commanders of DON organizations and users of DON IT must ensure all computers used for remote access have DoD approved antivirus and firewall protection that includes the capability for automated updates per references (e), (i), and (j). The most current definitions and updates for these applications must be loaded before a remote access session is established.

g. DON IT administrators /privileged users must comply with the following requirements when accessing DON IT from outside of the enclave:

(1) Once the DON organization determines the mission need for remote access, they must establish approved VPN connections using government-furnished equipment under their user accounts (with user privileges). All remote access to DON classified systems or networks must use NSA-approved COMSEC and keying material.

(2) After establishing a secure connection, elevate permissions to the appropriate level for conducting administrator tasks.

(3) Terminate connection when administrator tasks are complete.

(4) Safeguard information (i.e., do not access or display in an area where unauthorized persons are present) and control the equipment after connection termination per reference (x).

5. PKI Requirements

a. DON IT users must ensure encryption of CUI contained in Web server transactions using DoD PKI.

b. Users may only use software based certificates when the DON CIO or the appropriate DON Deputy CIO provides written certification of mission essentiality. This does not preclude the use of software certificates related to the DoD External Certificate Program, device/server software certificates, and software certificates used for group/role based functions.

c. General Officers/Flag Officers/Senior Executive Service members and their designated staff may use Alternate (ALT) tokens to maintain security and support senior level requirements. ALT tokens must be in accordance with the procedures in reference (y). Use of ALT tokens within the Secretariat staff must be approved by the DON CIO. The DON Deputy CIO (Navy) must approve their use by Navy staff, and the DON Deputy CIO (Marine Corps) for Marine Corps staff.