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

DOI
25 February 2020
FEB 2 5 2020

MEMORANDUM FOR DISTRIBUTION

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY

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

Department of Navy (DON) information technology (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 most critical information to threats, and increase costs through spillage and higher bandwidth requirements. We must change the cyber culture, take responsibility for cybersecurity, and practice good cyber hygiene. Maintaining cyber readiness is an all hands responsibility. The combined effect of recreational internet surfing and non-mission related high bandwidth intensive activities (e.g., streaming media such as movies or music, downloading images for personal use, etc.), impacts overall network performance, impedes critical business and mission needs and exposes our information systems to unnecessary vulnerabilities.

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 DON IT resources are being utilized in an acceptable manner and in accordance with this policy. Ensure your personnel are aware the DON uses tools to monitor user activity and implements varying levels of capacity/filtering restrictions. Communications made using DON IT and information stored on DON IT are not private, are subject to routine monitoring, interception, and search, and may be disclosed for any authorized government purposes.

This memorandum updates the Acceptable Use of DON IT Policy and cancels reference (a). This policy is a coordinated effort between the DON Chief Information Office (DON CIO) and the Office of the Deputy Under Secretary of the Navy (DUSN) as part of the DON's cyber/traditional security partnership for the protection of national security information, controlled unclassified information, and information systems.

The DON CIO point of contact for this policy is Ms. Jennifer Harper, 703-695-1983, Jennifer.A.Harper@navy.mil.

Aaron D. Weiss
Department of the Navy
Chief Information Officer

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY

Distribution:
VCNO
ACMC
ASN (RD&A)
ASN (M&RA)
ASN (EI&E)
ASN (FM&C)
DUSN (P)
OCMO
NCIS
CNR
CHINFO
DON/AA
DASN (RDT&E)
DASN (M&B)
DASN (E&LM)
DASN (C4I & SPACE)
DASN (AP)
DASN (UxS)
DNS
DMCS
OPNAV (N1/N2/N6/N3/N5/N4/N8/N9)
HQMC (DCI)
HQMC (IC4)
HQMC (DC P&R)
HQMC (DC, PP&O)
DON Deputy CIO (Navy)
DON Deputy CIO (Marine Corps)
FLTCYBERCOM/10THFLT
COMNAVAIRSYSCOM
COMNAVSEASYSCOM
COMNAVWARSYSCOM
COMNAVSUPSYSCOM
COMNAVRESFORCOM
COMNAVSPECWARCOM
COMNAVFACENGCOM
COMUSFLTFORCOM
COMMARFORCOM
COMPACFLT
COMUSNAVEUR/AF/C6F
COMUSNAVCENTCOM
COMNAVSO
COMOPTEVFOR
PEO (EIS)
PEO (C4I)

Subj: ACCEPTABLE USE OF DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY

ONR
ONI
NRL
NIA
CNIC
BUMED
BUPERS
DIRSSP
COMNAVDIST
COMNAVSAFECEN
USNA
FLDSUPPACT
NAVHISTHERITAGECOM
NETC
NAVPGSCOL
NAVWARCOL
MARCORSYSCOM
MARFORCYBER
MARCORLOGCOM
MCICOM
TECOM
MCRC
MCCS
MARFOREUR
MARFORPAC
MCIA
MCCDC
MCTSSA
MARFORRES
MARFORCOM
MARFORSOC
MARFORCENT
MCCOG

ENCLOSURE 1 – REFERENCES

(a) DON CIO Memorandum, Acceptable Use of Department of the Navy (DON) Information Technology (IT), 12 February 2016
(b) SECNAV MANUAL 5239.1 DON Information Assurance Manual, 1 November 2005
(c) DoD 5500.7R, Joint Ethics Regulatin (JER), Change 7, Section 2-301, 17 November 2011
(d) DoDI 8500.01, Cybersecurity, 14 March 2014
(e) SECNAVINST 5510.30C, Department of the Navy Personnel Security Program, 24 Jan 2020
(f) DoDM 5200.01 (Vol 4), DoD Information Security Program: Controlled Unclassified Information (CUI), Change 1, 24 February 2012
(g) SECNAVINST 3070.2, Operations Security, 5 May 2016
(h) SECNAVINST-5510.36B, Department of the Navy Information Security Program, 12 July 2019
(i) CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014
(j) NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, 15 Juanuary 2014
(k) CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities, 24 January 2012
(l) DODI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, 28 July 2017
(m) 5 CFR Part 1400 Designation of National Security Positions
(n) 5 CFR Part 731 Suitability
(o) DoDI 8170.01, Online Information Management and Electronic Messaging, 2 January 2019
(p) SECNAVINST 5510.34B, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives, 11 March 2019
(q) DoDD 5230.20, Visits and Assignments of Foreign Nationals, 22 June 2005
(r) UNSECNAV Memo, subject: Use of Personal Messaging Accounts to Conduct Official Business, 12 July 2019
(s) SECNAVINST 5210.8E, Department of the Navy Records Management Program, 17 December 2015
(t) CJCS M-6510.01B, Cyber Incident Handling Program, 10 July 2012
(u) OMB M-06-16, Protection of Sensitive Agency Information, 23 June 2006
(v) DoDI 5400.11, DoD Privacy and Civil Liberties Programs, 29 January 2019
(w) DoDI 1035.01, Telework Policy, 4 April 2012
(x) DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011

ENCLOSURE 2 – ACCEPTABLE USE OF DON IT

1. General Use
   a. DON IT users include every Sailor, Marine, civilian, contract support person, or foreign national with approved access to DON IT.
   b. DON IT is the collective term that encompasses all DON IT assets including, but not limited to: Information Systems (IS); applications; Operational Technology (OT); Platform IT (PIT); Industrial Control Systems (ICS); Supervisory Control and Data Acquisition (SCADA); Hull, Mechanical, and Electrical (HM&E) systems; Research, Development, Test, and Evaluation (RDT&E) Labs; IT products; IT services, Cloud Services; and any other IT asset per reference (b).
   c. DON IT users must observe all policies and procedures governing the secure operation and authorized use of DON IT.
   d. 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.
   e. 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 (c). Personal use must not adversely affect the performance of official duties or degrade network performance, and must be of reasonable duration and frequency as determined by commanding officers and supervisors. This includes personal communications that are most reasonably made during the work day (such as checking in with immediate family, scheduling doctor and auto or home repair appointments, brief Internet searches, conducting on-line banking, and distance learning). Non-emergency personal communications shall be made during personal time, such as after duty hours or lunch periods.
   f. 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.
   g. 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 prohibitied behaviors should be addressed to a supervisor or ethics officer.
   h. DON IT users may not use official email addresses to sign up for non-official online services (e.g., adult content).
   i. Commands shall ensure required background investigations are completed commensurate with the level of DON IT access a user requires, per references (d) and (e).
   j. All DON IT users shall have an approved System Authorization Access Request (SAAR) on file prior to being granted access to DON networks, systems or applications.

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

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

m. 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).

n. 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 (except for authorized use of Outlook Web Access (OWA)).

o. Users must not upload or download executable files of any type onto DON IT resources without the written approval of the local CS authority.

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

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

r. In accordance with reference (c), 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.

s. Users must mark and safeguard Controlled Unclassified Information (CUI) in accordance with reference (f). All CUI must be encypted prior to transmission on Non-classified Internet Protocol (IP) Router Network (NIPRNet).

t. Users must report all security incidents, including PII breaches, immediately in accordance with references (f), (g), and (h), and Command policy and procedures.

u. 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).

v. Users must protect Department of Defense (DoD)/DON Information and IT to prevent unauthorized access, compromise, tampering, exploitation, unauthorized or inadvertent modification, disclosure, destruction, or misuse.

w. Users must protect authenticators (e.g., passwords and personal identification numbers (PIN)) required for logon authenticatin at the same classification as the highest classification of the information accessed.

x. 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. Token will not be shared or left unattended and must be properly secured.

y. Users must ensure all information, programs, and other files are virus-checked prior to uploading them onto any DON IT resource.

z. 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.

aa. Commanders of DON organizations shall obtain formal authorization to interconnect Information Systems (IS) and networks per references (d), (i), (j), (k), and (l).

bb. DON organizations may use Internet based capabilities as defined in references (m), (n), (o), and other applicable policies.

cc. 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 (d), (e), (h), (i), (j), (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 requirement 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 Privacy Awareness training initially and annually.

c. DON IT users must complete derivative classification training prior to being granted access to DON classified IT in accordance with reference (h).

d. Users must complete DON approved Operations Security (OPSEC) courses within 30 days after receiving access to DON IT in accordance with reference (g). OPSEC training must include initial orientation and an annual refresher course. Completing the annual OPSEC refresher course is a condition that users must meet for continued use of DON IT.

3. Personal Messaging Accounts

a. In accordance with reference (r), existing law, DoD policy, and DON Policy, all DON officials and military and civilian employees must use their official DoD messaging accounts when conducting official DoD business with very limited exceptions.

b. Use of non-official email to conduct official business is only permitted in a rare circumstance that meets these combined three conditions in accordance with reference (o):

(1) Emergencies and other critical mission needs;

(2) When official communication capabilities are unavailable, impractical, or unreliable; and,

(3) It is in the best interests of DoD or other U.S. Government missions.

c. Under no circumstances should non-official messaging accounts, including but not limited to, e-mail, social media, mobile applications, cloud applications, or messaging applications be used for official business based on personal convenience or preference. Personal, non-official accounts may be used to participate in activities such as professional networking,

development, and collaboration related to, but not directly associated with, official mission activities as a DON official or military or civilian employee.

d. In the event that a DON Official or employee must use non-official email to conduct DON business, he or she must either
    (1) Copy his or her official messaging account at the time of transmission, or
    (2) Forward the communication to his or her official messaging account within 20 days from the date of transmission of the record per reference (s) and 44 U.S.C. § 2911.
    (3) When using non-official email, the sender must mitigate against transmitting non-public or controlled unclassified information including "For Official Use Only" (FOUO) and PII. Intentional violations may be the basis for disciplinary measures up to and including removal from Federal service.
e. Users shall not auto-forward official email from their DON email accounts to personal messaging accounts.

4. Outlook Web Access (OWA)

a. DON IT users may access OWA for unclassified official email using personally owned and other non-DoD computers. Users must:
    (1) Use public key infrastructure (PKI) authentication.
    (2) Handle, store, maintain and destroy all unclassified information in accordance with DoD and DON policies.
    (3) Immediately notify their commands of any information loss, theft or suspicious behavior of their system(s).
    (4) Protect the confidentiality, integrity and availability of DON email systems and information at all times.
    (5) 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. Government source software is available to support this requirement for all DON employees and contractors as described at https://infosec.navy.mil
    (6) 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.
    (7) Use Wireless Fidelity (WiFi) hotspots only if the connection and user complies with remote access requirements.
    (8) Ensure that no other wireless or Local Area Network (LAN) connection exists for the duration of the OWA session. Any other existing connections must be disabled for the duration of the session.
    (9) At the completion of an OWA session:
        i. Close all DON Email files.
        ii. Clear the web browser's cache.
        iii. Exit and close the browser.
        iv. Immediately turn off and reboot the computer.

4. Remote Access
   a. Commanders of DON organizations shall control remote access to DON IT per references (c), (d), (g), (j), (k), (s), (t), and (u).
   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 ISs and networks, including telework access, is mediated through a managed access control point, such as a remote access server in a demilitarized zone. Use encryption to protect the confidentiality of the session, per reference (d)
   d. Commanders of DON organizations must ensure authentication and confidentiality requirements for remote access sessions use National Security Agency (NSA) approved communications security (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 (d), (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 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 National Security Agency (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.

5. PKI Requirements
   a. Users must digitally sign all email.
   b. DON IT users must encrypt CUI contained in emails and web server transactions using DoD PKI per ref (f). Examples of this are attachments that contain personal identity or budget information.
   c. Users may only use software based certificates when the DON CIO or the appropriate DON Deputy CIO (DDCIO) 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.

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

I certify that I have completed the review of the DON Acceptable Use Policy and I understand that I will be held responsible for ensuring all rules are applied or my access to all information systems WILL be suspended.

DATE:		