



# Defense Health Agency **ADMINISTRATIVE INSTRUCTION**

**NUMBER 081**  
September 15, 2015

---

---

HIT/CSD

SUBJECT: Employee use of Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency Administrative Instruction (DHA-AI), based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (i), establishes procedures for DoD employees and Defense Contractors of the Defense Health Agency (DHA) (hereafter referred to as DHA personnel), on the proper use of DHA IT assets as authorized and/or privileged users.

2. APPLICABILITY. This AI applies to all DHA personnel requiring access to DHA IT resources, to include: assigned or attached Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary, or permanent duties at DHA to include regional and field activities (remote locations).

3. POLICY. It is DHA policy, pursuant to References (c) through (h), that DHA personnel will:

a. As authorized and/or privileged users, use DHA IT for official use and authorized purposes only.

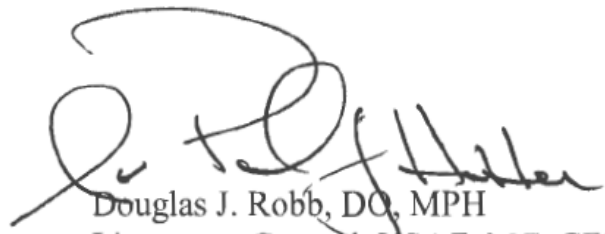
b. Provide consent to interception and monitoring of communications when using DHA IT.

c. Be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place IT at risk by not ensuring implementation of DoD system security requirements.

d. Use only a Common Access Card (CAC) to access DHA IT.

e. Complete Cyber Awareness training before access is granted to DHA IT and annually in order to retain access. Failure to comply with this policy will result in immediate termination of access to DHA IT in accordance with Reference (h).

4. RESPONSIBILITIES. See Enclosure 2
  
5. PROCEDURES. See Enclosure 3
  
6. RELEASABILITY. **Not cleared for public release.** This AI is available to DHA employees and contractor support personnel with CAC authorization on the DHA Intranet.
  
7. EFFECTIVE DATE. This AI:
  - a. Is effective upon signature.
  
  - b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with DHA Procedural Instruction 5025.01 (Reference (i)).



Douglas J. Robb, DO, MPH  
Lieutenant General, USAF, MC, CFS  
Director

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013
- (b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
- (c) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
- (d) DoD Instruction 8550.0, "Internet Services and Internet-Based Capabilities," September 11, 2012
- (e) DoD Manual 8570.01, "Information Assurance Workforce Improvement Program," December 19, 2005
- (f) DoD Regulation 5500.07, "Joint Ethics Regulation (JER)," August 1993
- (g) CJCS Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 11, 2011
- (h) DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004
- (i) DHA Procedural Instruction 5025.01, "Publication System," August 21, 2015

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, HEALTH INFORMATION TECHNOLOGY (HIT) DIRECTORATE. The Director, HIT Directorate, will:

- a. Develop, implement, maintain, and enforce a Cyber Security Program that protects DHA IT.
- b. Monitor DHA personnel's compliance with this AI, and control access to DHA IT.
- c. Terminate authorized user access for violations of DoD policy and this AI.
- d. Accept Joint Knowledge Online certification of annual Cyber Awareness training or Service components' Cyber Awareness training based on the current version of the Defense Information Systems Agency's Cyber Awareness Challenge.

2. DIRECTORS, DIRECTORATES, AND SPECIAL STAFF. The Directors, Directorates, and Special Staff will:

- a. Ensure that DHA personnel assigned to their organization complete initial and annual DoD Cyber Awareness training.
- b. Ensure that DHA personnel assigned to their organization use DHA IT in accordance with DoD policy (References (c)–(h)) and the procedures of this AI.

3. DHA PERSONNEL. DHA personnel will:

- a. Comply, as authorized users, with the procedures of Appendix I to Enclosure 3.
- b. Comply, as privileged users, with the procedures of Appendices I and II to Enclosure 3.
- c. Complete, as privileged users, the DHA IT Privileged User Access Agreement and Acknowledgment of Responsibilities in Appendix III to Enclosure 3.
- d. Provide evidence of DoD (or Service component equivalent) annual Cyber Awareness training certification upon assignment to DHA.

ENCLOSURE 3

PROCEDURES - APPENDIX I: AUTHORIZED USERS

1. REQUIREMENTS. DHA personnel will adhere to the following requirements for use of DHA IT:
  - a. Provide evidence of DoD (or Service component equivalent) Cyber Awareness training certificate as a condition of access to DHA IT, and complete DoD's Cyber Awareness training annually thereafter to maintain access in accordance with Reference (c).
  - b. Complete DD Form 2875, "System Authorization Access Request (SAAR)."
  - c. Immediately report all cybersecurity-related events, potential threats, and vulnerabilities to their Information System Security Officer (ISSO) or, in the absence of an ISSO, the Information System Security Manager (ISSM).
  - d. Digitally sign all e-mails that contain embedded hyperlinks and/or attachments by utilizing a DoD-approved Public Key Infrastructure.
  - e. Digitally sign and encrypt all e-mails containing Controlled Unclassified Information (CUI).
  - f. Protect terminals, workstations, other input/output devices, and resident data from unauthorized access.
  - g. Use only DHA-procured removable storage devices/flash media and follow Data at Rest instructions.
  - h. Obtain authorization (written approval or digitally signed e-mail) from their O-6/GS-15 Division Chief to use removable storage devices/flash media in support of operational mission essential requirements.
  - i. Obtain approval of the Authorizing Official (AO) or Authorizing Official's Designated Representative (AODR) to use removable storage devices/flash media in support of operational mission essential requirements.
  - j. Coordinate with the ISSM or ISSO on procedures to obtain a removable storage device/flash media and on the proper use and disposal of removable storage devices.
  - k. Contact network/enclave management support personnel for the procedures and processes for use of removable storage devices/flash media.
  - l. Encrypt all removable storage devices/flash media containing CUI.

- m. Do not attempt to connect personal wireless devices to DHA IT.
- n. Do not send CUI to personal e-mail addresses.
- o. Use DoD IT only for official or authorized purposes.
- p. Do not unilaterally bypass, strain, or test IT cybersecurity mechanisms.
- q. Do not introduce or use unauthorized software, firmware, or hardware on DHA IT.
- r. Do not relocate or change DHA IT equipment or the network connectivity of equipment without proper authorization.
- s. Observe DHA's policies and procedures governing the secure operation and authorized use of DHA IT.
- t. Encrypt all e-mails containing CUI, which includes, but is not limited to, personally identifiable information (PII) or protected health information (PHI). Do not use personal or commercial e-mail accounts for transmission of CUI, including PII or PHI data.
- u. Do not auto-forward e-mail(s) from a DoD/DHA e-mail account to personal or commercial e-mail accounts.
- v. Immediately notify their supervisor and the DHA Privacy and Civil Liberties Office of a suspected or actual information breach involving PII or PHI.
- w. Do not use commercial or personal e-mail accounts to conduct official business.
- x. Use non-mission-related contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal accounts, when such information is required for Internet-based Capabilities (IbC) personal accounts.
- y. Properly mark and classify information (e.g., e-mails, briefings, documents, or reports).
- z. Do not conduct official DoD communication in IbC personal accounts.
- aa. Do not disclose CUI and CUI that aggregates to reveal sensitive or classified information in IbC personal accounts.
- ab. Disclaim opinions in IbC personal accounts with the following statement: "The views presented are those of the individual and do not necessarily represent the views of the DoD or the DHA." (Reference (e)).
- ac. Avoid dissemination and discussion of non-public information in IbC personal accounts.
- ad. Protect DHA IT assets from theft, loss, or damage.

- ae. Use CACs to access DHA IT.
- af. Do not leave CACs unattended.

2. AUTHORIZED USE. DHA IT may be used for the authorized purposes of reasonable duration and frequency so as not to adversely affect the performance of official duties. Whenever possible, such use should be made during the employee's personal time, such as after duty hours or during lunch periods:

- a. E-mailing short messages to a relative or colleague.
- b. Accessing personal e-mail accounts.
- c. Announcing DHA-related activities (e.g., office luncheons, retirement or departure events, and holiday office parties).
- d. Making a medical, dental, auto repair, or similar appointment.
- e. Accessing the Internet for professional development purposes.
- f. Authorizing a financial transaction.
- g. Reading news or professional journals.
- h. Accessing personal IbC accounts, such as Facebook, Twitter, etc.

3. PROHIBITED USE. DHA IT may not be used to support the following unauthorized activities:

- a. Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment.
- b. Fundraising activities not sanctioned by DHA.
- c. Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity, including campaign fundraising.
- d. Use of a DHA network as a staging ground or platform to gain unauthorized access to other systems.
- e. Attempting to circumvent, disable, or compromise DHA security features and authentication measures.
- f. Accessing, creating, downloading, viewing, storing, copying, or transmitting materials

related to illegal gambling, illegal weapons, and/or any other prohibited or illegal activities.

g. Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to terrorist activities, sexually oriented, or racist materials.

h. Participating in “spamming”; that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

i. Participating in “letter-bombing”; that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient’s use of e-mail.

j. Downloading shareware/freeware software, malicious code, or executable programs (e.g., .EXE, .COM, .BAT, or script.INI files). (Note: Usage of Network File System open-source software is permitted with a risk assessment and AO/AODR approval).

k. Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

l. Using the system for personal financial gain, such as advertising, solicitation of services, sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker).

m. Posting DHA information to external newsgroups, bulletin boards, or other public forums without authority.

n. Sending, whether initiating or replying to, inappropriate messages or messages containing inappropriate language.

o. Accessing sites known for hacker attacks or hacker activity.

p. Opening e-mail attachments from unknown or questionable sources.

q. Transmitting CUI, including PII and PHI in e-mails and via the Internet without ensuring appropriate security controls (e.g., use of Federal Information Processing Standards’ compliant encryption algorithms) are in place.



APPENDIX II: PRIVILEGED USERS

PRIVILEGED USERS' REQUIREMENTS. In addition to the requirements of Enclosure 3, Appendix I, privileged users will:

- a. Configure and operate IT within the authorities vested in them according to DoD cybersecurity policies and procedures, and notify the responsible ISSO or, in the absence of an ISSO, the responsible ISSM, of any changes that might impact security postures.
- b. Complete the DHA IT Privileged User Access Agreement and Acknowledgment of Responsibilities within Appendix III to Enclosure 3 and provide to the ISSM.
- c. Be fully qualified per Reference (c), as well as trained and certified to DoD baseline requirements to perform their Information Assurance duties.
- d. Complete specified computing environment training.
- e. Ensure that if IT and its storage media containing PHI or PII will be used by others without a need-to-know, the information is removed in such a way that the data may not be reconstructed (e.g., degauss, smelt, incinerate, disintegrate, or pulverize), thereby rendering stored information unrecoverable.

APPENDIX III: DHA IT PRIVILEGED USER ACCESS AGREEMENT AND  
ACKNOWLEDGEMENT OF RESPONSIBILITIES

Date: \_\_\_\_\_

1. I understand there are two DoD Information Systems (ISs), classified (SIPRNET) and unclassified (NIPRNET), and that I have the necessary clearance for privileged access to DHA [specify which IS the privileges are for]. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.
2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the [IS NAME]. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers who are not authorized [IS NAME] access.
3. I understand that I am responsible for all actions taken under my account(s), root, or otherwise. I will not attempt to “hack” the network or any connected ISs or gain access to data to which I do not have authorized access.
4. I understand my responsibility to appropriately protect and label all output generated under my account, including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files.
5. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate [IS NAME] Information System Security Manager (ISSM) or Information System Security Officer (ISSO). I will NOT install, modify, or remove any hardware or software (e.g., freeware/shareware and security tools) without written permission and approval from the [IS NAME] ISSM or ISSO.
6. I will not install any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).
7. I will not add/remove any users’ names to the Domain Administrators, Local Administrator, or Power Users group without the prior approval and direction of the [IS NAME] ISSM or ISSO.
8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the [IS NAME] local area networks.
9. I understand that I am prohibited from the following while using DoD IT:
  - a. Introducing classified information into a NIPRNET environment.

b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.

c. Storing, accessing, processing, or distributing Classified, Proprietary, Controlled Unclassified Information, For Official Use Only, or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

f. Engaging in prohibited political activity.

g. Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker).

h. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers and charitable fund raisers, without approval).

i. Gambling, wagering, or placing of any bets.

j. Writing, forwarding, or participating in chain letters.

k. Posting personal home pages.

l. Any other actions prohibited by DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004 (Reference (h)) or any other DoD issuances.

10. I understand that personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

11. I understand that if I am in doubt as to any of my roles or responsibilities, I will contact the [IS NAME] ISSM or ISSO for clarification.

12. I understand that all information processed on the [IS NAME] is subject to monitoring. This includes e-mail and browsing the Web.

13. I will not allow any user who is not cleared access to the network or any other connected

system without prior approval or specific guidance from the [IS NAME] ISSM.

14. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission-related functions.

15. I will not use any DoD/Components' owned Information System (IS) to violate software copyright by making illegal copies of software.

16. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day-to-day network communications.

17. I understand that failure to comply with the above requirements will be reported and may result in the following actions:

- a. Revocation of IS privileged access;
- b. Counseling;
- c. Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution;
- d. Disciplinary action, discharge, or loss of employment; and
- e. Revocation of security clearance.

18. I will obtain and maintain required certification(s), according to DoD Manual 8570.01, "Information Assurance Workforce Improvement Program," dated December 19, 2005 (as amended), and the certification provider, to retain privileged system access.

INFORMATION SYSTEM NAME \_\_\_\_\_

NAME \_\_\_\_\_

SIGNATURE \_\_\_\_\_

Date \_\_\_\_\_

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
AODR	Authorizing Official's Designated Representative
CAC	Common Access Card
CUI	Controlled Unclassified Information
DHA	Defense Health Agency
DHA-AI	Defense Health Agency Administrative Instruction
HIT	Health Information Technology
IbC	Internet-based Capabilities
IS	Information System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
PHI	protected health information
PII	personally identifiable information

PART II. DEFINITIONS

authorized purposes. Personal use within specified limits as permitted by an appropriate level supervisor.

authorized user. Any appropriately cleared individual with a requirement to access a DoD IS for performing or assisting in a lawful and authorized governmental function.

CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. Includes: For Official Use Only, Law Enforcement Sensitive, DoD Unclassified Controlled Nuclear Information, PII, PHI, and Limited Distribution.

Defense Contractor. Any individual, firm, corporation, partnership, association, or other legal non-federal entity that enters into a contract directly with DoD or a DoD Component to furnish services, supplies, or both, including construction. Subcontractors are excluded.

DHA IT. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display,

switching, interchange, transmission, or reception of data or information by DHA. For purposes of the preceding sentence, equipment is used by DHA if the equipment is used by DHA directly or is used by a contractor under a contract with DHA which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

DoD Employee.

Any DoD civilian officer or employee (including special government employees) of any DoD Component (including any non-appropriated fund activity).

Any Active Duty Regular or Reserve military officer, including warrant officers.  
Any Active Duty enlisted member of the Army, Navy, Air Force, or Marine Corps.

Any Reserve or National Guard member on Active Duty under orders issued pursuant to Title 10, United States Code.

Any Reserve or National Guard member while performing official duties or functions under the authority of either Title 10 or Title 32, United States Code, or while engaged in any activity related to the performance of such duties or functions, including any time the member uses his/her Reserve or National Guard of the United States title or position, or any authority derived there from.

Any faculty member in a civil service position or hired pursuant to Title 10, United States Code, and any student (including a cadet or midshipman) of an academy, college, university, or school of DoD.

Consistent with labor agreements and international treaties and agreements, and host country laws, any foreign national working for a DoD Component except those hired pursuant to a defense contract.

IbC. All public information capabilities or applications available across the Internet from locations not directly or indirectly controlled by DoD or the Federal Government (i.e., locations not owned or operated by DoD, another federal agency, or by contractors or others on behalf of DoD or another federal agency).

IT. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a

**product.** The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

**official use.** Uses that directly further the interests of the DoD and the duties prescribed for the individual position.

**privileged user.** An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions.