Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 086
January 6, 2017

HIT/OCTO

SUBJECT: E-mail Address Certificates on Common Access Cards (CACs)

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency-Administrative Instruction (DHA-AI), based on the authority of References (f) and (g), and in accordance with the guidance of References (a) through (e), establishes the Defense Health Agency's (DHA) procedures for complying with the assignment of organization e-mail addresses, which have been provided by government entities, on CACs issued after the latest policy effective date of Reference (c). By making this information available, DHA will be able to ensure that only e-mail address certificates provided by government entities identified in Reference (c) are assigned to new CACs at the time of issuance.

2. APPLICABILITY. This DHA-AI applies to all CAC users that support the DHA, to include: assigned, attached, or detailed Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA, regardless of whether or not they are on the DHA-network.

3. POLICY IMPLEMENTATION. It is DHA's policy pursuant to References (b) and (c) that CACs issued, reissued, or replaced after the latest policy effective date of Reference (c) will require an organization e-mail address certificate, which has been provided by a government entity, at the time of issuance in order to be able to leverage email certificate functions, such as digital signature and encryption. If such an e-mail address is not available at the time of issuance, the CAC will still be issued with an e-mail certificate containing a blank e-mail address. Capabilities afforded by a CAC that do not require an approved e-mail certificate for authentication will still function. CACs issued, reissued, or replaced prior to the policy effective date of Reference (c) are grandfathered in until such time the CAC is reissued, issued, or replaced after the policy effective date. Additional guidance on the protection of sensitive information in electronic mail is provided as Reference (d).

4. RESPONSIBILITIES. See Enclosure 2

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Not cleared for public release**. This DHA-AI is available to users with CAC authorization on the DHA Intranet.

7. EFFECTIVE DATE. This DHA-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 (e)).

For R.C. BONO
VADM, MC, USN
Director

Enclosures
1. References
2. Responsibilities
3. Procedures
Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Memorandum, "Designation of Department of Defense Enterprise Email as an Enterprise Service for the Joint Information Environment," September 5, 2013[1]

(b) DoD Manual 1000.13 – Volume 1, "DoD Identification (ID) Cards: ID Card Life-Cycle," January 23, 2014

(c) Defense Human Resources Activity Headquarters Memorandum, "Enforcing Department of Defense Government E-mail Address Assignment at Common Access Card Issuance," April 27, 2016[2]

(d) Tricare Management Activity Memorandum, "Updated Guidelines on Protection of Sensitive Information in Electronic Mail," November 17, 2010.

(e) DHA-Procedural Instruction 5025.01, "Publication System," August 21, 2015

(f) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013

(g) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013

[1] More information regarding DEE can be found at http://www.disa.mil/Services/Enterprise-Services/Applications/DoD-Enterprise-Email.

[2] More information regarding this reference can be found at www.dmdc.osd.mil or by contacting 571-372-1088.

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will:

a. Maintain oversight activities and management controls to ensure compliance with this DHA-AI.

b. Oversee coordination of the implementation for those DHA personnel identified in Enclosure 3 of this DHA-AI.

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

a. Provide guidance establishing the DHA's procedures for complying with the use of organization e-mail addresses, which have been provided by government entities, being assigned on CACs issued after the latest policy effective date of Reference (c).

b. Coordinate revision of IT-related requirement and procedure changes to this DHA-AI, as needed.

3. CONTRACTING OFFICER (KO). The KO will:

a. Ensure requirements are consistent with the contract requirements.

b. Direct the COR to perform responsibilities.

4. CONTRACTING OFFICER 'S REPRESENTATIVE (COR)/PROGRAM MANAGER (PM). The COR/PM will receive direction from the KO, or be delegated the authority, to:

a. Coordinate with the contract's respective Facility Security Officer (FSO) for compliance with the DoD and Defense Human Resources Activity's requirements.

b. Ensure timely coordination with the Global Service Center (GSC) throughout the process of obtaining a Defense Enterprise Email (DEE) account.

5. CONTRACTOR FSO. The Contractor FSO will:

a. Ensure all new CACs are assigned organization e-mail addresses, which have been provided by government entities, at time of issuance.

b. Work with the COR/PM to submit a CAC owner's name and Electronic Data Interchange Personal Identifier (EDIPI) to the GSC for Defense Enterprise Email (DEE) account creation requests.

6. <u>SUPPORT REPRESENTATIVES, GSC</u>. The GSC will:

a. Act on requests to create and configure DEE accounts.

b. Send acknowledgment of account creation to FSO/COR/PM/user along with instructions on how users should create or update their Defense Enrollment Eligibility Reporting System (DEERS) information.

c. Assist DEE account holders with accessing DEE webmail using Outlook Web Access (OWA) at https://web.mail.mil.

7. <u>CAC OWNER</u>. The CAC Owner, will:

a. Update and maintain CAC e-mail address certificates per Enclosure 3.

b. Update and maintain "work contact info GAL" per Enclosure 3.

ENCLOSURE 3

PROCEDURES

1. SCENARIO A FOR CACs ISSUED, REISSUED, OR REPLACED BEFORE THE LATEST POLICY EFFECTIVE DATE OF REFERENCE (C). Existing CACs will not be affected, disabled, or terminated (regardless of whether or not they have an organization e-mail address provided by a government entity).

a. The CAC will still work and existing privileges will not be lost (i.e., e-mails, GAL, using it to access CAC-enabled sites such as SharePoint, digital signatures, e-mail encryption, etc.).

b. Once the CAC or contract expires, an organization e-mail address provided by a government entity will be required in order to obtain an e-mail certificate on new/renewed CACs, per Scenario B described below.

2. SCENARIO B FOR CACs ISSUED, REISSUED, OR REPLACED AFTER THE LATEST POLICY EFFECTIVE DATE OF REFERENCE (C). When issuing, reissuing, or replacing a CAC, only an organization e-mail address provided by a government entity can be used to obtain an e-mail certificate on the CAC. Approved e-mail extensions are provided in the Attachment of Reference (c). The DHA's preferred course of action is to obtain a Defense Enterprise Email (DEE) with a mail.mil email address. To obtain a contractor's mail.mil e-mail address, a CAC/EDIPI is required.

If such an e-mail, from the Attachment of Reference (C), does not exist, the CAC will still be issued but with a blank e-mail certificate. Once an e-mail address is issued by a government entity, the CAC's e-mail certificate can be updated, and CAC capabilities that require e-mail certificate authentication will be activated, such as digital signatures and e-mail encryption.

a. The COR/PM will schedule a meeting with the respective contractor's FSO to gather CAC user information.

b. The FSO develops and submits a list of the user's e-mail and EDIPI, which is located on the back of his/her CAC, to the COR/PM.

c. The COR/PM routes information to the GSC at DHA.ITCallCenter@mail.mil requesting that a DEE account be created for each user.

d. The GSC creates a DEE account for each user.

e. The GSC sends FSO's acknowledgment of account creation along with instructions on how users should create or update their DEERS/Real-Time Automated Personnel Identification System Online profiles.

f. The FSO forwards account information to COR/PM.

g. The COR/PM forwards new account information and instructions to user.

h. The user then:

(1) Signs in to the link below (do not select the DoD EMAIL certificate option): https://www.dmdc.osd.mil/self_service/

(2) Selects ‘Change CAC Email’ within ‘CAC Maintenance’.

(3) Updates the email address on their CAC to reflect their DEE (@mail.mil account. This will create the DoD Certificates needed for digitally signing and encryption (may take up to 72 hours).

(4) Updates their GAL properties at the link below: https://www.dmdc.osd.mil/milconnect/and select “Update work contact info (GAL).”

NOTE: The amount of time required to obtain a DEE account is contingent upon the independent steps performed by the parties outlined in the steps above.

(5) Accesses their DEE mail accounts at https://web.mail.mil.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CAC	Common Access Card
COR	Contracting Officer's Representative
DEE	Defense Enterprise Email
DEERS	Defense Enrollment Eligibility Reporting System
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
EDIPI	Electronic Data Interchange Personal Identifier
FSO	Facility Security Officer
GAL	Global Address Lookup
GSC	Global Service Center
KO	Contracting Officer
OWA	Outlook Web Access
PM	Program Manager

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this DHA-AI.

CAC. The CAC is a standard identification method for active duty U.S Defense personnel, DoD civilian employees, and eligible DoD contractor personnel. It is the principal card used to enable physical access to controlled spaces, and provides access to defense computer networks and systems.

Contractor employee. An employee of a firm, or individual under contract or subcontract to the DoD, designated as providing services or support to the Department.

a. Internal contractor: DHA-assigned contractors that have DHA network access.

b. External contractor: DHA-assigned contractors that do not have DHA network access.

DHA. DHA is a joint, integrated Combat Support Agency that enables the U.S. Army, Navy, and Air Force Medical Services to provide a "medically ready force and ready medical force" to Combatant Commands. DHA's mission is to achieve greater integration of direct and purchased health care delivery systems in order to accomplish the Department's Quadruple Aim.