**DEPARTMENT OF THE ARMY**
**OFFICE OF THE SECRETARY OF THE ARMY**
**107 ARMY PENTAGON**
**WASHINGTON DC 20310-0107**

Office, Chief Information Officer/G-6

SAIS-AOI

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Department of Defense Enterprise Email (DEE) Never Accessed and Idle Account Policy

1. References:

a. Army Regulation (AR) 25-1, Army Information Technology, 25 July 2013.

b. Memorandum, Under Secretary of the Army, 12 December 2013, subject: Department of Defense Enterprise Email (DEE) Address Use for Common Access Card (CAC) Certificates.

c. Memorandum, Chief Information Officer/G-6, 11 November 2013, Enterprise Email Journaling.

d. Army Cyber Command Execute Order (EXORD) 2011-070, Army Unclassified Enterprise E-Mail Migration.

2. Purpose. This policy will establish a rule set by which the Army manages DEE accounts that have not been accessed or that remain idle for a prescribed period of time (see enclosure).

3. Background. In 2010, the CIO/G-6 implemented DEE to improve email capabilities and reduce costs. In July 2013, the Army completed its migration to DEE. The migration effectively moved existing Army accounts to Defense Information Systems Agency (DISA) infrastructure, resulting the creation of more than 1.4 million DEE accounts. On 6 January 2014, the Army implemented the policy cited in reference b. Since that implementation, the Army has considered Basic Class DEE accounts a basic issue item for all Army personnel; thus, they are not de-provisioned or deleted as long as the user maintains an active Common Access Card.

4. Scope. This policy applies to Army DEE accounts on the NIPRNet and SIPRNet. Email accounts that are subject to journaling are excluded from this policy.

5. Policy. Effective immediately upon signature, all Army DEE entitlement managers (EMs) and group managers (GMs) are directed to use the business rules, processes

and definitions listed in the enclosure to categorize and manage never accessed and idle DEE accounts.

6. Policy Compliance. The CIO/G-6, in coordination with Army Cyber Command, Program Executive Officer Enterprise Information Systems and DISA, will implement and enforce this policy change for the Army.

7. Policy Exceptions. Exceptions to policy are approved at the local level on a case-by-case basis by EMs through their GMs. EMs and GMs should use sound discretion when managing accounts, as they are subject to user and/or command unique mission requirements.

8. Policy expiration. This policy remains in effect until it is rescinded or superseded.

9. The point of contact for this action is LTC Guy DeWees: (703) 614-7287 (DSN 224) or guy.m.dewees.mil@mail.mil. Questions also may be sent to usarmy.pentagon.hqda-cio-g-6.mbx.sais-aoi@mail.mil.

Digitally signed by FERRELL.ROBERT.SILAS.1028607268
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=FERRELL.ROBERT.SILAS.1028607268
Date: 2015.08.29 23:50:57 -04'00'

Encl

ROBERT S. FERRELL
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers

(CONT)

DISTRIBUTION: (CONT)
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade
Commandant, U.S. Army War College

CF:
Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army
Commander, U.S. Army Cyber Command
Commander, Second Army

Step 1: Identify and characterize all email accounts within your organization

"Never accessed" and "idle" accounts are terms used to describe the operating status of a personal or organizational email account. De-provision and delete are methods by which accounts that are no longer in use are disabled and removed from the service.

a. A never-accessed account is an account that has never been accessed or transacted in.

b. An idle account is a user or organizational account that has not been used for a period of 60 days or more.

c. An account that is de-provisioned is disabled. No transactions in or out will occur. The account will be tagged "de-provisioned" and any email sent to a de-provisioned account will result in a Non-Delivery Report. The account can be re-provisioned (and email recovered) for up to 120 days after the de-provisioning action.

d. The email from a de-provisioned account will be deleted by DISA on the 121st day following de-provisioning. That email will then be non-recoverable.

e. A Non-Person Entity (NPE) account is primarily an organizational mailbox or organizational calendar, but the term also includes distribution lists, and the mailbox/calendar for audio/video conference bridges, rooms, vehicles, portable audio-visual devices, and other equipment.

f. A non-Army user mailbox is an Army-paid-for user mailbox for an individual that is assigned to a DoD component outside the Army but for which the Army has a responsibility to provide the email service (for example, USN personnel assigned to an organization for which the Army is the executive agent, USAF weather personnel supporting an Army airfield, DoD civilians or contractors working on an Army installation, etc.).

Step 2: Once identified, analyze those accounts identified as never accessed / idle for corrective action

Step 3: Take appropriate prescribed corrective action identified below

**Table 1. NIPR Accounts**

| Account Type | Characterization | 60 Day Action | 180 Day Action |
|---|---|---|---|
| Army Basic Class | Never Accessed/Idle | None | None |
| Non-Army User (Army Business Class) | Never Accessed/Idle | De-provision | N/A |
| Army User (Business Class) | Never Accessed | Reduce to Basic | N/A |
| Army Business Class | Idle | None | Reduce to Basic |

| Account Type | Characterization | 60 Day Action | 180 Day Action |
|---|---|---|---|
| Non-Person Entity* | Never Accessed/Idle | Delete | N/A |

* Applies to group mailboxes only

a. On NIPR, individual business class DEE accounts for Army personnel that are never accessed will be downgraded to Basic Class after 60 days. If a Business Class account of an Army person remains idle for 180 days, it will be downgraded to Basic Class.

b. Business class accounts for non-Army personnel will be de-provisioned if never accessed or idle for 60 days.

c. NIPR NPEs will be deleted if never accessed or idle for 60 days.

**Table 2. SIPR Accounts**

| Account Type | Characterization | 60 Day Action | 180 Day Action |
|---|---|---|---|
| Army Business Class | Never Accessed/Idle | De-provision | N/A |
| Non-Person Entity* | Never Accessed | Delete | N/A |
| Non-Person Entity* | Idle | None | Delete |

* Applies to group mailboxes only

d. On SIPR, individual business class DEE accounts for all personnel that are never accessed or idle will be de-provisioned after 60 days.

e. SIPR NPEs will be deleted if never accessed for 60 days or idle for 180 days.

f. NOTE FOR BOTH NIPR AND SIPR ACCOUNTS: An account that has been de-provisioned can be re-provisioned for up to 120 days after the de-provisioning date with no loss of email. After the 120 days, the user's mailbox is deleted and the email cannot be recovered for the user, but the contents will be managed in accordance with the Army CAPSTONE email disposition schedule. If re-provisioned prior to the 120 days, the account will contain the data that was in the account when it was de-provisioned. If email deletion occurs and the user still has a valid CAC, an entitlement manager can re-provision the user with a new (empty) mailbox account using the Defense Enterprise Provisioning Online portal.