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-CB

AUG 11 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Privileged Access to Army Information Systems and Networks

1. References.

a. Army Regulation (AR) 25-2, Information Assurance (IA), 23 March 2009.

b. AR 25-1, Army Information Technology (IT), 25 June 2013.

c. Department of Defense (DoD) 8570.01-M, IA Workforce Improvement Program, 24 January 2012.

2. Purpose. This memorandum clarifies Army policy and directs actions associated with requesting, receiving and monitoring Soldiers, civilians, contractors, vendors and any other individuals with privileged access (i.e., users with elevated privileges, privileged users) to Army information systems and networks.

3. Applicability. The policy and directed actions in this memorandum apply to the active Army, the Army National Guard / Army National Guard of the United States, and the U.S. Army Reserve.

4. Policy.

a. Commands and other Army activities will maintain the ability to nominate Soldiers, civilians, contractors and other individuals as candidates for privileged access via signed (physical or digital) Appointment Orders/Appointing Letters. These must:

1) Designate the IT position category based upon the maximum level of privileged access required for the candidate, in accordance with AR 25-2: “IT-I” (i.e., privileged access); “IT-II” (i.e., limited privileged access); or “IT-III” (i.e., limited privileged access to individual systems / power user / general user).

2) Designate the information assurance (IA) workforce category/specialty and level of the candidate per DoD 8570.01-M, in accordance with the position’s listed

requirements and the position's functions (i.e., actions/duties). For example: "IAT-II", "IAM-I" and "CND-IR".

3) Specify the functions to be performed by the candidate that require privileged access.

a) Functions must be specified at the Unclassified level and should not contain specific server names, IP addresses or other potentially sensitive information.

b) Describe each function with sufficient detail to establish that privileged access is necessary to perform the function.

c) Include the specific access rights needed to perform each function.

d) Identify each function as "above-baseline", or one of the following delivered IT support services per AR 25-1: baseline, enhanced, mission-funded or mission-unique. This can be determined by the Network Enterprise Center (NEC), the IT service provider or the funding source for the position/services.

e) An example of specification of functions is: "Mission-funded: Full privileged access required on non-enterprise servers of the 36th Infantry Division in order to install operating system patches and software patches, and to conduct backups."

b. Each candidate for privileged access must complete and sign (physically or digitally) a Privileged-level Access Agreement (PAA) and a Non-Disclosure Agreement (NDA). The PAA and NDA may be combined into a single document.

c. Templates for the Appointment Orders, PAAs and NDAs are available in the 'Documents' section of the Army Training & Certification Tracking System (ATCTS), located at https://atc.us.army.mil. Commands and other Army activities may expand upon the content in the templates.

d. Commands and other Army activities must upload completed/signed Appointment Orders, PAAs and NDAs to ATCTS, located at https://atc.us.army.mil.

e. For enterprise and provider-managed user accounts, NECs or designated service providers will authorize and deny granting of privileged access. For other user accounts, the appointed IA Manager (IAM) who oversees the IA security program will authorize and deny granting of privileged access.

1) Authorization and denial decisions will be documented.

2) The rationale for denials will be provided to the requesting Command or other Army activity, giving them an opportunity to resubmit the request.

3) Disagreements regarding enterprise and provider-managed user accounts will be escalated to the Director of the NEC/service provider. For other user accounts, disagreements will be escalated to the appointed IA Program Manager (IAPM).

4) The final arbiter of any disagreement concerning authorization or denial of privileged access will be the appointed Authorizing Official (AO)/Designated Approving Authority (DAA) of the Army Signal Command (Theater) or other area of responsibility.

f. The specific NECs or designated service providers responsible for authorizing, denying and managing users' privileged access, when not clear and agreed upon, will be determined by the Theater Signal Commander.

g. Commands and other Army activities will notify and coordinate with the respective NEC, IT service provider or IAM to revoke the privileged access of any user whose functions no longer require such access.

h. Commands and other Army activities will promptly remove or update the Appointment Orders in ATCTS when privileged access has been denied or is no longer required.

i. Commands and other Army activities will promptly notify and coordinate with Security Managers upon changes to an individual's privileged access to ensure continuity of required suitability investigations and contract security requirements, in accordance with the IT Position Category and any classification/caveats.

5. Directed actions.

a. Commanders, Program Managers, Theater Signal Commands, Signal Brigades, NECs, designated service providers and IA personnel will ensure enforcement of this policy.

b. Commands and other Army activities with users who have privileged access will promptly upon signing of this memorandum:

1) Revalidate users with privileged access, now and on a quarterly basis, to ensure that such access is commensurate with: current mission requirements, the user's position level, and a need for the user to perform functions that specifically require privileged access.

2) Incorporate procedures to revoke promptly the privileged access of any user account as soon as the user position and/or functions no longer require such access.

a) Prior to departure, disable privileged user accounts for all individuals who are no longer employed, have been reassigned or will be on extended absence.

b) Reduce overlapping functions and privileges, as appropriate, to meet mission needs.

c) Promptly notify and coordinate with the respective NEC, IT service provider or IAM to accomplish user account changes.

d) Promptly notify and coordinate with Security Managers to ensure continuity of required suitability investigations and contract security requirements, in accordance with the IT Position Category and any classification/caveats.

3) Review current Appointment Orders to ensure full compliance with this memorandum and update non-compliant Appointment Orders within 60 days.

4) Remove or update the Appointment Orders in ATCTS when privileged access has been denied or is no longer required.

5) Ensure that all individuals with privileged access have completed and signed (physically or digitally) Appointment Orders, a PAA and an NDA uploaded to ATCTS.

c. NECs, designated service providers and IAMs will:

1) Revoke the privileged access of user accounts for which documentation is not fully compliant within one year of this memorandum's being signed. Provide notice of this revocation to the individual with the user account and his associated Command or other Army activity.

2) Ensure that new requests for privileged access are in full compliance with this memorandum.

3) Ensure that all individuals with privileged access have completed and signed (physically or digitally) Appointment Orders, a PAA and an NDA.

4) Promptly revoke the user account privileged access upon notification by the Command or other Army activity that such access is no longer required.

d. Theater Signal Commands will coordinate with their NECs and IT service providers to oversee this policy and its associated process via quarterly reviews of documentation (e.g., appointment orders, PAAs, NDAs, decisions) for the request and authorization or denial of privileged access. For Army activities outside a Theater Signal Command area of responsibility, oversight will be provided by the appointed

AO/DAA and the associate IA personnel.

6. Effectiveness of this policy will be determined via the above oversight reviews and cyber security/information assurance compliance assessments. This policy will be reviewed for update annually.

7. The point of contact for this memorandum is Ms. Melissa Hicks, CIO/G-6 Cyber Security Directorate: melissa.c.hicks.civ@mail.mil or (703) 545-1604.

FERRELL.ROBERT.SILAS.1028607268
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: 2014.08.11 17:35:10 -04'00'

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
- 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
(CONT)

DISTRIBUTION (CONT):
Commandant, U.S. Army War College
Commander, Second Army

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