



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CI

8 April 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Reserve Network Account Management Policy

1. References:

- a. Army Regulation (AR) 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.
- b. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), <https://iase.disa.mil/stigs/Pages/index.aspx>.
- c. United States Army Chief Information Officer (CIO)/G-6 Cyber Directorate Information Assurance Best Business Practice (IA BBP) 05-PR-M-0002, IA Training and Certification, Version 5.0, 10 April 2012.
- d. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (updated 22 January 2015).
- e. JTF-GNO CTO 07-015, Public Key Infrastructure (PKI) Implementation, Phase 2, 11 December 2007.
- f. ARCYBER & 2A OPORD 2016-033, Implementation of Documentation of Privileged Users, 17 February 2016.
- g. United States Army Reserve Command (USARC) CIO/G-6 Network Account Management Standard Operating Procedure (SOP), <https://xtranet/usarc/g6/ITG/G6%20SOPs/Forms/AllItems.aspx>.

2. Purpose: This policy enforces user account management for all United States Army Reserve (USAR) managed networks (unclassified and classified). All users are required to request an account using the Army Reserve Account Management and Provisioning (ARAMP) application in order to access USAR networks.

3. Applicability: This policy applies to all USAR managed network users.

AFRC-CI

SUBJECT: United States Army Reserve Network Account Management Policy

4. Policy:

a. User account management is a critical component of an effective enterprise network security posture. User accounts will be reviewed periodically by the Data Center Core Services Team. In accordance with AR 25-2, paragraph 3-3a(10), any account that has been inactive for more than 45 days will be disabled. Accounts that have been inactive for 90 days will be deleted. Privileged-level accounts will also be disabled after 45 days of inactivity and deleted after 90 days of inactivity.

b. User and privileged-level account activity is recorded as follows:

(1) Users log into their accounts from workstations directly connected to the network or by authorized USARC managed wireless access points.

(2) Users log into their accounts via a virtual private network.

(3) Users log into Outlook Web Access to access their email over the Internet.

(4) Users send or receive email via BlackBerry/iPhone transmission.

c. Common Access Card (CAC)/Public Key Infrastructure (PKI) User-Based Enforcement (UBE) policies will be applied to all user accounts on USAR managed networks (unclassified and classified). All information system and user account policies will be configured to ensure: two-factor authentication, PIN requirements, and time-based screen lockout features in accordance with applicable DISA STIGs, AR 25-2, IA BBP, and USARC Active Directory Naming Conventions. The Authorizing Official (AO) reserves the authority to disable UBE on a case-by-case basis.

d. Paragraph 3-3a(13) of AR 25-2 states that privileged-level access account users will maintain and use two separate accounts for network resource access, one for their privileged-level access and functions and a separate general user, non-privileged level account for routine administrative work. This documents and proves the concept of least privilege, allowing only authorized access for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. All privileged-level access accounts on USAR networks will have an Alternate Smart Card Logon (ASCL) token provisioned to the account and are required to login using the ASCL.

e. All USAR network accounts (privileged and non-privileged) will be requested using the ARAMP application and approved and managed using USARC CIO/G-6 Network Account Management SOP processes (reference g).

AFRC-CI

SUBJECT: United States Army Reserve Network Account Management Policy

f. Shared user accounts (accounts where two or more people log in with the same user identification) are not permitted on USAR managed networks or systems. Shared user accounts do not provide adequate identification, authentication, nonrepudiation, or individual accountability for system access and resource usage. Unapproved shared accounts must be documented with the Information System Security Officer (ISSO)/Information System Security Manager (ISSM) and the account must be removed from the system.

EXCEPTION: Shared accounts, such as required by an application, may be approved by the organization. Application accounts are requested through ARAMP and must follow a strict approval process. Application accounts will not be allowed on USAR managed networks before final adjudication and approval is achieved. Application accounts must be documented with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

g. All accounts are subject to independent audit review, either by an automated process or by the ISSM or other authorized auditing agencies at the direction of the AO, USARC CIO/G-6, or Cybersecurity Operations Branch Chief.

h. USARC Cybersecurity Operations Branch will perform quarterly reviews of privileged level accounts per OPOD 2016-033 by generating a Privileged-Level Access Agreement (PAA) report in the Army Training and Certification Tracking System (ATCTS), and providing to the ISSM.

5. Effective Date. This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.

6. The point of contact for this policy is the undersigned at (910) 570-8653 or kimberly.m.register.civ@mail.mil.

2 Encls

1. Memo, OSA, Aug 09 2018
2. Memo, USARC, 11 March 2019

Kimberly M. Register
Chief, USARC CIO/G-6 Cybersecurity
Program Management (ISSM)

DISTRIBUTION:
(see next page)

AFRC-CI

SUBJECT: United States Army Reserve Network Account Management Policy

DISTRIBUTION:

GEOGRAPHIC COMMANDS:

1 MSC

7 MSC

9 MSC

63 DIV (R)

- USAG-FHL

81 DIV (R)

- USAG-Fort Buchanan

88 DIV (R)

- USAG-Fort McCoy

99 DIV (R)

- ASA-Dix

FUNCTIONAL COMMANDS:

3 MCDS

76 ORC

79 TSC

200 MP CMD

311 SC(T)

335 SC(T)

377 TSC

412 TEC

416 TEC

807 MCDS

ARAC

ARCD

AR-MEDCOM

LEGAL CMD

MIRC

USACAPOC(A)

75 TNG CMD (MC)

80 TNG CMD (TASS)

83 US ARRTC

84 TNG CMD (UR)

85 USAR SPT CMD

108 TNG CMD (IET)

USAR SPT CMD (1A)

(CONT)

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy

DISTRIBUTION: (CONT)

AREC/ARET:

USARPAC
ARNORTH
ARSOUTH
ARCENT
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

CF:

USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy



Office, Chief Information Officer / G-6

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

AUG 09 2018

SAIS-ZS

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Information Assurance (IA) Military Workforce Limited Set of System Administration Privileges

1. References:

- a. DoD 8570.01-M, Information Assurance Workforce Improvement Program, Chapter 3 (IA Workforce Technical Category), Change 4, 10 November 2015.
- b. Department of Defense Directive 8140.01, Cyberspace Workforce Management, Change 1, 31 July 2017.

2. The Department of Defense mandates that all IA certification programs include training, industry-standard certifications (e.g., CompTIA Security+) and work experience that enable execution of IA functions and tasks. Prior to obtaining industry certification, Soldiers must acquire the knowledge, skills and abilities to execute tasks and responsibilities required by their assigned duty positions. Certified military IA professionals validate and supervise on-the-job training performance of Information Assurance Task (IAT) Level 1 functions (Reference A).

3. Currently, this IA certification process induces unacceptable risks and unwarranted burdens within our formations. Specifically, the levels of certification required to perform routine information assurance and signal tasks at the tactical level are not optimal. For example, when a Soldier reports to his or her unit of assignment and does not possess the required industry-standard certification, the unit cannot utilize the Soldier for any task that requires elevated network access. This includes adding or removing peripherals and associated applications, thus impacting readiness.

4. This memorandum modifies and eases the burden by providing general-purpose users (25Bs/Us/Ns) a limited set of system access privileges, while simultaneously mitigating operational shortfalls in order to sustain the tactical network. It also includes guidance for IAT Level 1 Functions, Task T-I.3 (provide end-user IA support for all computing environment operating systems, peripherals and applications).

5. At the conclusion of Advanced Individual Training (AIT), Soldiers awarded the 25B10, 25N10 or 25U10 Military Occupational Specialty (MOS) have been trained in

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy

SAIS-ZS
SUBJECT: U.S. Army Information Assurance Military Workforce Limited Set of System Administration Privileges

basic technical and networking skills commensurate with future IAT Level 1 functions. In consideration of this, and in order to allow entry-level personnel to gain practical experience, the Army is modifying IAT Level 1 Task T-1.3 to permit those in ranks E-1 through E-4 to install operating systems, peripherals and applications without obtaining industry-standard certifications.

6. Execution. As the Army's Authorizing Official, in accordance with reference a, I designate the training received during AIT for 25B10, 25N10 and 25U10 MOSs as sufficient for entry-level IAT Level 1 Task T-1.3 functions. Industry certification is no longer necessary for E-1 through E-4 personnel in IAT Level 1 positions to perform this task. Therefore, these personnel will be granted a limited set of system administration privileges that are commensurate with their skill level, knowledge base and designated work roles to install peripherals and associated applications per the following:

- a. Soldiers must possess the knowledge, skills and abilities to execute the tasks and responsibilities required by their assigned position and verified by the chain of command.
- b. Either upon assignment to a Non-Commissioned Officer position that specifically requires an industry IA certification (as annotated by the Table of Equipment (TOE), Modified TOE or Table of Distribution and Allowances) or receipt of appointment orders to an additional-duty IA position (as defined by Army Regulation 25-2, Chapter 3), Soldiers must meet industry-standard IA certification requirements corresponding to the IAT Level 1 functions defined in reference a within six months of assuming the IA position. Once the certification is achieved, Soldiers will be upgraded to the category of "IA Workforce" in the Army Training and Certification Tracking System.
- c. Commanders at all levels retain the authority to recognize a Soldier's leadership and technical potential, and may approve a Soldier's seeking commercial certification prior to promotion to E-5 as an exception to paragraph 6b of this memorandum. Unit commanders will retain the authority to grant or revoke a limited set of system administration privileges based upon mission requirements and the individual Soldier's knowledge, skills and abilities.
- d. Commands will need to coordinate with their local Network Enterprise Centers (NECs) to restrict the scope of privileged access through Active Directory in order to monitor and control network activity.
- e. Per this memorandum, NEC directors and the Department of the Army Inspector General will accept AIT training for 25B10, 25N10 and 25U10 Soldiers (ranks E-1 to E-4) as sufficient to grant a limited set of system administration privileges, commensurate with the Soldier's skill level, knowledge base and designated work roles, to perform entry-level IAT Level 1 Task T-1.3 functions.

AFRC-CI

SUBJECT: United States Army Reserve Network Account Management Policy


SAIS-ZS

SUBJECT: U.S. Army Information Assurance Military Workforce Limited Set of System Administration Privileges

7. Duration. This policy is effective upon signature and will be re-evaluated two years after the date of this memorandum.

8. This policy supersedes existing policies dated 19 July 2011 and 17 April 2014, respectively.

9. The CIO/G-6 point of contact for this memorandum is SGM Travis L. Cherry: (703) 697-7494 or travis.l.cherry4.mil@mail.mil.



BRUCE T. CRAWFORD
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 Cyber 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
- U.S. Army Human Resources Command
- U.S. Army Financial Management Command

(CONT)

AFRC-CI

SUBJECT: United States Army Reserve Network Account Management Policy

SAIS-ZS

SUBJECT: U.S. Army Information Assurance Military Workforce Limited Set of System
Administration Privileges

DISTRIBUTION: (CONT)

U.S. Army Marketing and Engagement Brigade
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency

CF:

Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CII

11 March 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Service Account Policy for United States Army Reserve Network

1. References:

- a. DoD Directive (DoDD) 8140.01, Cyberspace Workforce Management, Change 1, 31 July 2017.
- b. United States Army Chief Information Officer (CIO)/G-6 Cyber Directorate Information Assurance Best Business Practice (IA BBP) 05-PR-M-0002, IA Training and Certification, Version 5.0, 10 April 2012.
- c. DoD 8570.01-M, Information Assurance Workforce Improvement Program, Change 4, 10 November 2015.
- d. Army Regulation (AR) 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.
- e. Memorandum, Office of the Secretary of the Army, Aug 09 2018, subject: U.S. Army Information Assurance (IA) Military Workforce Limited Set of System Administration Privileges.

2. Purpose: This policy provides guidance on requesting and approving service accounts.

3. Applicability: This policy applies to:

- a. Army Reserve organizations or personnel who are requesting service accounts.
- b. Information System Security Managers (ISSM) who approve service account requests.

4. Policy:

- a. Army Reserve personnel who submits an Army Reserve Account Maintenance and Provisioning (ARAMP) request for a service account on behalf of his or her organization will submit a justification memorandum to United States Army Reserve Command (USARC) Chief Information Officer (CIO)/G-6 Cybersecurity upon request.

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy

AFRC-CII
SUBJECT: Service Account Policy for United States Army Reserve Network

Once the ARAMP request is received, a USARC CIO/G-6 Cybersecurity representative will email the requestor asking for the justification memorandum. The request will be approved entirely at Cybersecurity's discretion.

b. Justification memoranda will be stored on the share drive at:
[\\AR\Enterprise\CyberSecurity\Historical\Service Account Justification Memos.](#)

5. Responsibilities: ISSMs will ensure full compliance with this memorandum.

6. Effective Date: This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.

7. The point of contact for this policy is the undersigned at (910) 570-8653 or kimberly.m.register.civ@mail.mil.

REGISTER.KIMBERLY.MARIE.10
37987553

Digitally signed by
REGISTER.KIMBERLY.MARIE.1037987553
Date: 2019.03.11 15:51:33 -04'00'

KIMBERLY M. REGISTER
Chief, USARC CIO/G-6 Cybersecurity
Program Management (ISSM)

DISTRIBUTION:

GEOGRAPHIC COMMANDS:

1 MSC
7 MSC
9 MSC
63 DIV (R)
- USAG-FHL
81 DIV (R)
- USAG-Fort Buchanan
88 DIV (R)
- USAG-Fort McCoy
99 DIV (R)
- ASA-Dix

FUNCTIONAL COMMANDS:

3 MCDS
76 ORC
79 TSC
200 MP CMD
311 SC(T)
335 SC(T)
377 TSC
(CONT)

AFRC-CI
SUBJECT: United States Army Reserve Network Account Management Policy

AFRC-CII
SUBJECT: Service Account Policy for United States Army Reserve Network

DISTRIBUTION: (CONT)

412 TEC
416 TEC
807 MCDS
ARCD
AR-MEDCOM
ARAC
LEGAL CMD
MIRC
USACAPOC(A)
75 TNG CMD (MC)
80 TNG CMD (TASS)
83 US ARRTC
84 TNG CMD (UR)
85 USAR SPT CMD
108 TNG CMD (IET)
USAR SPT CMD (1A)

AREC/ARET:

USARPAC
ARNORTH
ARSOUTH
ARCENT
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

CF:

USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies