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

AFRC-CI

27 November 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Assignment of Privileged User Accounts

1. References:

a. Department of Defense (DoD) Directive 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, Information Assurance (IA) Training and Certification, Version 5.0, 30 March 2012.

c. DoD 8570.01-M, Information Assurance Workforce Improvement Program, Change 4, 10 November 2015.

d. Army Regulation 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.

e. United States Army Reserve Command (USARC) CIO/G-6, Assignment of Privileged User Accounts Standard Operating Procedure (SOP), https://xtranet/usarc/g6/ITG/G6%20SOPs/Forms/AllItems.aspx.

2. Purpose: This policy establishes guidance for granting administrator privileges to personnel accessing United States Army Reserve (USAR) managed networks (unclassified and classified).

3. Applicability: This policy applies to all personnel requesting administrator privileges on USAR managed networks.

4. Policy: In order to qualify for network administrator privileges, personnel must have a mission essential need for privileges and meet specific training and certification requirements. The unit Information Assurance Support Officer will ensure full compliance with this policy. Personnel who are serving in dual roles (Military, or DoD Civilian or Contractor) must comply with the most stringent training and certification policy of the two roles.

a. Cyber Awareness Training: All cyber security personnel must successfully complete initial and annual refresher DoD Cyber Awareness Challenge Training at https://ia.signal.army.mil/DoDIAA/default.asp.

b. Wide Network Security Force (WNSF) Training: All cybersecurity personnel must successfully complete initial one-time WNSF courses at https://iatraining.us.army.mil/.

(1) WNSF - Portable Electronic Devices and Removable Storage Media v2.0
(2) WNSF - Phishing Awareness v2.0
(3) WNSF - Personally Identifiable Information (PII) v2.0
(4) WNSF - Safe Home Computing

c. Cyber Security Fundamentals Training (formerly known as Information Assurance Fundamentals): All cybersecurity personnel must successfully complete initial one-time Cyber Security Fundamentals training at https://ia.signal.army.mil/IAF/default.asp.

d. Cybersecurity Contractor Workforce: Contractor personnel must obtain the appropriate baseline certification and Computing Environment (CE) certification prior to approval of any administrator privileged account. All Contractors must release their baseline certifications to DoD and be validated by the Defense Manpower Data Center (DMDC). The validation must appear in the individual's Army Training and Certification Tracking System (ATCTS) profile prior to a privileged-level account being granted.

(1) DMDC website link https://milconnect.dmdc.osd.mil/milconnect/.

(2) ATCTS website link https://atc.us.army.mil/iastar/index.php.

e. Types of Privileged Accounts

(1) Information Assurance Technical (IAT) Levels: All personnel must attain a baseline and CE certification for the operating system(s) and/or security-related tools/devices supported within 6 months of IA appointment (with the exception of Contractors). If supporting multiple tools and devices, IAT certified personnel must obtain CE certifications for all the tools and devices they are supporting.

(2) Appointed IA Manager (IAM) personnel are not to perform technical duties unless an additional duty appointment has been signed by an approved signature authority. IAM positions that also perform IAT functions must obtain the appropriate technical level certification and must complete all IAT level requirements prior to being granted unsupervised privileged access.

(3) Organizational Unit Administrator (OU Admin) privileges are defined as membership in the domain administrators group or the global domain administrators group. The OU Administrator is a member of his or her organizational unit group and is an unsupervised privileged account.

(4) System Administrator (SA) privileges are defined as membership in the local administrators group or the global domain administrators group. The SA management of all member servers within the server OU is an unsupervised privileged account.

(5) The unit commander or the next higher level commander in the unit chain of command is the approval authority for granting administrator privileges (enclosure 1).

f. Levels of access and security clearance requirements:

(1) OU Admin/SA privileges will be granted only to individuals who meet the following criteria. Individuals with the following privileges require a minimum security clearance of Secret:

(a) The individuals' duty appointment orders must state their position title and OU Admin or SA duties. Example: An individual's primary duty is network management, i.e., a minimum of 90 percent of their duty time is spent installing, configuring, maintaining, and managing the hardware, software, communications, and security of network resources. The duty appointment orders (enclosure 1) would state Network Management as the position title.

(b) The individuals are at least an IAT-II level. They must obtain the appropriate training and baseline and CE certification prior to being engaged in OU Admin/SA activities. Personnel will follow the matrix in enclosure 2 to align the appropriate baseline certification to their IAT level. Based on their position, personnel will align the appropriate CE certifications with the security-related tools/devices they support. Minimum training requirements are listed in the IA Training and Certification Best Business Practices (reference 1b).

(c) Proof of Certification and Training: Copies of training certificates and related documents shall be maintained on file for each assigned administrator and network security person. These files will be uploaded to ATCTS (https://atc.us.army.mil/iastar/index.php) and maintained by the unit training officer, or administrative staff, as appropriate. Files will be readily available for command inspection.

(2) Requirements exist for various other levels of access involving privileges that may impact the security configuration of the network or specific network resources. Minimum training requirements must be met prior to granting these privileges. The individual's duty appointment orders (enclosure 1) must state the administrator's personnel security standards (IT-I, IT-II, or IT-III) and your IA category and level (IAT-I, IAT-II, or IAT-III or IAM-I, IAM-II, or IAM-III), a list of baseline and CE requirements (CEs are for IAT and not IAM), and a summary of the functions to be performed. These requirements must be obtained within 6 months of the date on the duty appointment orders (excluding Contractors). Individuals with the following privileges require a minimum security clearance of Secret:

(a) Individuals whose responsibility is limited to the management of a computer and a user account (IAT-I) may be added to the Local Account Operators Group as the following: Print Management (PrtMgt), Desk Management (DeskMgt), and Helpdesk. Minimum training requirements are listed in the IA Training and Certification Best Business Practices (reference 1b).

(b) Individuals whose responsibility is limited to the management of a specific local server, Training Administrator (TrngAdmin), or web server (IAT II) may be added to that server's local administrators group. Minimum training requirements are listed in the IA Training and Certification Best Business Practices (reference 1b).

(c) 25B/D/U with Supervised Privileged Access is reserved for military members in the rank of E1 through E4 who hold the Military Occupational Specialty (MOS) 25B (Information Technology Specialist), 25D (Cyber Network Defender), or 25U (Signal Support Systems Specialist) and have successfully completed Advanced Individual Training (AIT). These users must upload their AIT certificate to ATCTS, as well as list a supervisor on their account that is DoD 8570 compliant for IAT-II access or above. This will allow these administrators to work as IAT-I under supervision. These administrators will have until they reach the rank of E5 to become baseline and CE certified at the required IAT level for their position.

5. Effective Date: This policy is effective upon signature and it will remain in effect until this document is revised or superseded.

6. The point of contact for this memorandum is Mrs. Kimberly Register, Chief, USARC G-6 Cybersecurity Program Management Division, kimberly.m.register.civ@mail.mil or (910) 570-8653.

2 Encls
1. Appointment Orders Template
2. DoD Baseline Certifications

DENIS L. GIZINSKI
Chief Information Officer
Deputy Chief of Staff, G-6

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
(CONT)

DISTRIBUTION: (CONT)
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
(CONT)
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

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

Office Symbol

Date

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Appointment of Cybersecurity Personnel or Cybersecurity Support Personnel

1. Effective immediately, the following individual is appointed to perform cybersecurity duties/functions for the organizational unit (OU) indicated below:

a. Position Title: OU Administrator

b. Organizational Unit (OU): (e.g., DIVEAST, USARC, DIT080)

c. Name: LAST NAME, FIRST NAME MI
Grade: (e.g., GS-13, O-4, E-8)
Civilian Job Specialty Code/Military Occupational Specialty/Functional Area: (e.g., 2210, 25B, 53A)
Personnel Security Standards (IAW AR 25-2, para 4-14): IT-I
Information Assurance (IA) Category and Level (IAW DoD 8570.01-M): IAT-II

2. Authority:

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

b. Department of Defense (DoD) 8570.01-M, Information Assurance Workforce Improvement Program, Change 4, 10 November 2015.

3. Purpose: To perform cybersecurity functions and duties per paragraph 3 of AR 25-2 and DoD 8570-1.M and as directed in paragraph 6b below.

4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement, or discharge.

5. Special Instructions:

a. Register in the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil).

b. Complete required cybersecurity training and certification for category/level.

c. Complete USAR Form 75-1-R (Test) (Army Reserve Network (ARNet) Privileged-Level Access and Acknowledgement of Responsibilities Agreement), which is available at https://arg1web/pubs/forms/Pages/default.aspx; upload a copy to your ATCTS profile.

d. Complete USAR Form 75-R (Test) (Army Reserve Acceptable Use Policy (AUP)), which is available at https://arg1web/pubs/forms/Pages/default.aspx; upload a copy to your ATCTS profile.

e. Upload your completed Computing Environment (CE) training or certification to your ATCTS profile. You must complete [Enter the CE training or certification that is required for the position. The CE will be reviewed by the USARC Information Assurance Manager (IAM) or Information Assurance Program Manager (IAPM), and if not sufficient, the request for a privileged level account will be denied. Please delete the brackets and the information enclosed within the brackets prior to publishing the appointment orders.]

f. You must release your certificate and it must be validated by Defense Manpower Data Center (DMDC) within your ATCTS profile prior to being granted privileged-level access. This action must be completed prior to applying for a privileged-level access account within Army Reserve Account Maintenance Provisioning (ARAMP).

6. Functions to be performed:

a. IT Functions Service Category: Mission-funded, baseline

b. Functions to be performed: [Example: Full privileged access is required for all Active Directory Objects, Users, and Computers in order to apply new images and Security Technical Implementation Guides (STIGS) and to actively manage information systems (notebooks, laptops, and desktops), printers, multi-functional devices, and scanners within the OU identified in paragraph 1b above. Please delete the brackets and the information enclosed within the brackets prior to publishing the appointment orders.]

Office Symbol
SUBJECT: Appointment of Cybersecurity Personnel or Cybersecurity Support Personnel

7. The point of contact for this memorandum is [Enter individual's name (including military rank or civilian prefix), position, name@mail.mil or telephone number. Please delete the brackets and the information enclosed within the brackets prior to publishing the appointment orders.].

FIRST X. LAST
RANK [Company Commander], BRANCH
Duty Title

DISTRIBUTION
1 – Individual
2 – Duty Appointment File

CF:
1 – Organization G-6
1 – Individual ATCTS Profile

DoD Approved Baseline Certifications

Table AP3.T2 DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+CE CCNA-Security Network + CE SSCP	CCNA-Security GICSP GSEC Security+ CE SSCP	CASP CE CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH GCIA GCIH GICSP SCYBER	CEH GICSP SSCP	CEH ~~CSIH~~ GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CISA GSNA	CISM CISSP-ISSMP	

( )

ARMY STAFFING FORM For use of this form, see AR 25-50; the proponent agency is AASA.	1. TRACKING NUMBER	2. TODAY'S DATE (YYYYMMDD) 20171120	3. SUSPENSE DATE (YYYYMMDD) 20171124
4. OFFICE SYMBOL	5. SUBJECT Assignment of Privileged User Accounts Policy		

6. ROUTING:	Initial	Date

POC _____ *(Rank, Name, Phone)* DIR _____

COMMENTS:

7. EXECUTIVE SUMMARY / ACTION MEMORANDUM

Key Points

- This policy applies to all personnel requesting administrator privileges on USAR managed networks. All cyber security personnel must successfully complete initial and annual refresher DoD Cyber Awareness Training.
- All Cybersecurity personnel must successfully complete initial one-time WNSF courses - 4 total. All Cybersecurity personnel must successfully complete initial one-time Cyber Security Fundamentals training
- Cybersecurity Contractor Workforce: Contractor personnel must obtain the appropriate baseline certification and Computing Environment (CE) certification prior to approval of any administrator privileged account.

Ref:

Encl: TAB A: CIO/G6 Form 5 Routing Sheet
TAB B: Assignment of Privileged User Accounts Policy

1. Purpose:
This policy establishes guidance for granting administrator privileges to personnel accessing United States Army Reserve (USAR) managed networks (unclassified and classified).

2. Discussion:

In order to qualify for network administrator privileges, personnel must have a mission essential need for privileges and meet specific training and certification requirements. The unit Information Assurance Support Officer will ensure full compliance with this policy. Personnel who are serving in dual roles (Military, or DoD Civilian or Contractor) must comply with the most stringent training and certification policy of the two roles.

3. Recommendation:
If you have any questions or concerns about the information on this sheet, please contact Tanya Carrero 910-570-8339 or at tanya.m.carrero2.ctr@mail.mil.

APPROVED ____ **DISAPPROVED** ____ **NOTED** ____ **SEE ME** ____ **COMMENT** ____

8. LEAD AGENCY STAFF COORDINATION			TRACKING NUMBER:	
TITLE	INITIAL	TYPE OR PRINT NAME		DATE (YYYYMMDD)
Deputy	DB	Mr. Denis Gizinski		20171120
PRINCIPAL				
ACTION OFFICER (Name/Title/Phone Number/E-mail)		Mrs. Kimberly Register, CPMD Chef (910) 570-8653, kimberly.m.register.civ@mail.mil		
FILE LOCATION:				
SACO's NAME (Name/Title/Phone Number/E-mail)		MAJ Angella Beji, Info System Officer (910) 570-8651, angella.m.beji.mil@mail.mil		
RECOMMENDATION FOR STAFF PRINCIPAL:				

9. STAFF COORDINATION

CONCUR	NON-CONCUR	AGENCY	NAME (TITLE, LAST NAME)	PHONE	DATE (YYYYMMDD)	REMARKS
☐	☐		Mr. Matt Hoerner	910-570-8653		
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					
☐	☐					

10. REMARKS: ☐ RETURNED REQUESTING ADDITIONAL INFORMATION/CLARIFICATION