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

AFRC-CI

15 November 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Reserve Managed Network Violations Policy

1. References:

a. Army Regulation (AR) 380-67, Personnel Security Program, 24 January 2014.

b. AR 380-5, Department of the Army Information Security Program, 31 October 2000.

c. United States Army Chief Information Officer (CIO)/G-6 Cyber Directorate Information Assurance Best Business Practice (IA BBP) 06-PR-M-0003, Privileged Level Access Agreement, 3 November 2006.

d. Department of Defense (DoD) Instruction (DoDI) 8500.01, Cybersecurity, 14 March 2014.

e. DoD Directive (DoDD) 5500.07-R, Joint Ethics Regulation, 17 November 2011.

f. AR 25-1, Army Information Technology, 4 December 2008.

g. AR 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.

h. United States Army Reserve (USAR) 75-R (TEST), Army Reserve Acceptable Use Policy (AUP) for Access to CLASSIFIED/ UNCLASSIFIED Systems, 1 August 2008.

i. DoDI 3020.41, Contractor Personnel Authorized to Accompany the U.S. Armed Forces, 20December 2011.

2. Purpose: This policy defines authorized and unauthorized use of information systems and devices on USAR managed networks (unclassified or classified), as well as administrative actions for violation of this policy. This policy is designed to prevent network security violations (NSVs) and cross domain violations (CDVs).

3. Applicability: This policy applies to:

a. All personnel with access to information systems and devices used on USAR managed networks.

b. All information technologies used to input, process, store, display, or transmit information, regardless of classification or sensitivity.

4. Definitions:

a. Network security violations (NSVs) include a broad category of events that include, but are not limited to:

(1) Mishandling or exposure of classified information on lower classified networks.

(2) Improper or unauthorized data transfers between systems or networks reported as CDVs.

(3) Attempts to use or attach equipment or devices not authorized for connection to USAR managed networks.

(4) Attempts to use or install unauthorized software on USAR managed networks.

(5) Unauthorized attempts to access, collect, or harvest data for which an individual does not possess the appropriate clearance level.

(6) Any deliberate attempts to circumvent network access controls designed to protect sensitive or classified information.

b. Cross domain violations (CDVs) occur when an unaccredited or unauthorized information system or device is placed on a network. CSV examples include:

(1) Classified domain to unclassified domain (i.e., connecting a Secure Internet Protocol Router (SIPR) device to Non-Secure Internet Protocol Router (NIPR).

(2) Unclassified domain to classified domain (i.e., connecting a NIPR device to SIPR).

(3) Use of unauthorized removal storage media (RSM), charging of privately owned portable electronic devices (PEDs), to include iPod/iPhone, MP3 players, and BlackBerry smartphones.

c. Portable electronic devices (PEDs) are laptop computers, iPod/iPhone, Blackberry, or PDAs.

d. RSM include thumb drives (i.e., memory sticks, flash drives, Universal Serial Bus (USB) drives), pen drives, or external USB drives, floppy disks, CD/DVD, or photo flash cards that can store data, or any other electronic media that can be attached to, inserted in, plugged into or connected via USB, firewire, or wirelessly to a computer or information systems for the purpose of storing and/or transmitting data.

5. Policy:

a. All users of information systems and devices on USAR managed networks are required to meet the personnel security standards (i.e., favorable background investigation), read and sign USAR Form 75-R (TEST) (reference 1h), and receive training prior to gaining access to the device and/or network. Users must successfully complete required training, which includes the following:

(1) DoD Cyber Awareness Training (https://cs.signal.army.mil)

(2) Wide Network Security Focus (WNSF) training, to include:

(a) Phishing Awareness, Version 2

(b) Personally Identifiable Information (PII), Version 2

(c) Portable Electronic Devices and Removable Storage Media, Version 2

(d) SAFE Home Computing

b. To maintain access, users must successfully complete DoD Cyber Awareness Training, and read and sign USAR Form 75-R (TEST) (reference 1h) annually.

c. All mobile computing devices and removable media encrypted with an approved data-at-rest solution will be authorized by the United States Army Cyber Command (ARCYBER).

d. All authorized RSM must be marked with the appropriate level of classification using the GSA Standard Form sticker (i.e., SF 710, SF 707). Once used on a specific network, such as NIPR, SIPR, or CENTRIXS-K, devices must be marked appropriately and used only on the specified network. Government RSM will follow USAR Removable Media Standard Operating Procedure.

e. Unauthorized use of Army information systems include the following:

(1) Use of information systems that adversely reflects on the DoD or the Army, such as involving sexually explicit e-mail, accessing sexually explicit web sites, pornographic images including virtual computer-generated pornographic images, chain e-mail messages, unofficial advertising, soliciting, or selling via e-mail.

(2) Use of information systems for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policies, or personal use that promotes a particular religion or faith.

(3) Use of information systems that violate other Army policies or public laws including, but not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

(4) Political transmission that advocates the election of particular candidates for public office.

(5) Use of an Army information system for purposes that could directly or indirectly cause congestion, delay, or disruption of service to any computing facilities, or cause unwarranted or unsolicited interference with other personnel's use of the information system. Such uses include, but are not limited to, the use of the information system to:

(a) Create, download, store, copy, transmit, or broadcast illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.

(b) Spam to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(c) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients in order to interfere with the recipient or recipient's use of e-mail.

(d) Broadcast unsubstantiated virus warnings from sources other than System Administrators.

(e) Broadcast unofficial e-mail messages to large groups of e-mail users.

(f) Employ (Install) for personal use applications using streaming data (audio or video), malicious logic and virus development software and/or tools, files, unlicensed software, games, web altering tools/software, and other software that may cause harm to Government-owned computers and telecommunications systems.

f. Use of privately owned PEDs and/or RMS on DoD networks is explicitly prohibited. Sensitive DoD related information will not be stored on privately owned devices, or storage media, except when authorized.

g. Violation of this policy will result in forfeiture of user network privileges. All personnel (i.e., to include those in Information Assurance Management or Information Assurance Technical roles) found in violation of DoD, Army, and/or USAR regulations and/or policies will forfeit their user/privileged-level access as per the conditions set forth within the Acceptable Use Policy and the Privileged Level Access Agreement. Commanders may take action in accordance with the Uniform Code of Military Justice (UCMJ) when personnel violate DoD, Army, and/or USAR regulations and policies. Any incident that is criminal in nature will be reported to the Military Police (MP) and Criminal Investigation Department (CID).

(1) On the first offense, users found in violation of DoD, Army, and/or USAR policies listed in the references will forfeit their network access privileges for 1 week, successfully complete DoD Cyber Awareness Training (https:/lcs.signal.army.mil), and read and sign their AUP agreement. Upon approval of the ISSM, network access privileges will be reinstated.

(2) On the second offense, users found in violation of DoD, Army, and/or USAR policies listed in the references will forfeit their network access privileges for 2 weeks, successfully complete DoD Cyber Awareness Training (https://cs.signal.army.mil), and read and sign their AUP agreement. Upon approval of the ISSM, network access privileges will bereinstated.

(3) On the third offense, users found in violation of DoD, Army, and/or USAR policies listed in the references will forfeit their network privileges permanently.

(4) The United States Army Reserve Command (USARC) Authorizing Official will address all appeals to reinstate computer/network access privileges if they are removed for violation of this policy.

(5) For any network violation, an 0-7 or above in the chain of command will submit a memorandum to verify the individual completed all requirements and the mitigation action the unit will take to ensure the activity does not happen again before reactivating the individual's account.

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 Mrs. Kimberly Register, Chief, USARC CIO/G-6 Cybersecurity Program Management Division, (910) 570-8653 or kimberly.m.register.civ@mail.mil.

DENIS L. GIZINS
Chief Info ation Officer
USARC De uty 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
79TSC
200 MP CMD
311 SC{T)
(CONT)

DISTRIBUTION: (CONT)
335 SC(T)
377 TSC
412 TEC
416 TEC
807 MCDS
ARAC
ARCO
AR-MEDCOM
LEGAL CMD
MIRC
USACAPOC(A)
75 TNG CMD (MC)
80 TNG CMD (TASS)
83 USARRTC
84 TNG CMD (UR)
85 USAR SPT CMD
108 TNG CMD (IET)
USAR SPT CMD (1A)

AREC/ARET:
USARPAC
ARNORTH
ARSOUTH
ARGENT
AFRICOM
CENTCOM
USAREUR
USARAF
8THARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
Ill CORPS
XVIII ABC
USASOC
EUCOM
SOCOM
(CONT)

DISTRIBUTION: (CONT)

COPY FURNISH:
USARCXOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies

ARMY STAFFING FORM
For use of this form, see AR 25-50; the proponent agency is MSA.

1. TRACKING NUMBER

2. TODAY'S DATE *(YYYYMMDD)*
20171106

3. SUSPENSE DATE *(YYYYMMDD)*
20171110

4. OFFICE SYMBOL

5. SUBJECT
United States Army Reserve Managed Network Violations Policy

6. ROUTING: Initial **Date**

POC *(Rank, Name, Phone)* DIR

COMMENTS:

7. EXECUTIVE SUMMARY/ ACTION **MEMORANDUM**

Key Points

- This policy is designed to prevent network security violations (NSVs) and cross domain violations (CDVs).
- This policy applies to: All personnel with access to information systems and devices used on USAR managed networks.
- This policy applies to: All information technologies used to input, process, store, display, or transmit information, regardless of classification or sensitivity.

Ref:

Encl:TABA: CIO/G6 Form 5 Routing Sheet
TABB: United States Army Reserve Managed Network Violations Policy

1. Purpose:
This policy defines authorized and unauthorized use of information systems and devices on USAR managed networks (unclassified or classified), as well as administrative actions for violation of this policy.

2. Discussion:
All users of information systems and devices on USAR managed networks are required to meet the personnel security standards (i.e., favorable background investigation), read and sign USAR Form 75-R (TEST) (reference 1h), and receive training prior to gaining access to the device and/or network.

To maintain access, users must successfully complete DoD Cyber Awareness Training, and read and sign USAR Form 75-R (TEST) (reference 1h) annually.

All mobile computing devices and removable media encrypted with an approved data-at-rest solution will be authorized by the United States Army Cyber Command (ARCYBER).

All authorized RSM must be marked with the appropriate level of classification using the GSA Standard Form sticker (i.e., SF 710, SF 707). Once used on a specific network, such as NIPR, SIPR, or CENTRIXS-K, devices must be marked appropriately and used only on the specified network. Government RSM will follow USAR Removable Media Standard Operating Procedure.

3. Recommendation:

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

(   )

8. LEAD AGENCY STAFF COORDINATION | TRACKING NUMBER:

TITLE	INITIAL	TYPE OR PRINT NAME	ryyf J oDl
Deputy		Mr. Denis, Gizinski	
PRINCIPAL		t/ ·,)	

ACTION OFFICER C .:.; .:-;. C;-· _:-.,·. .· Mrs. Kimberly Register, CPMD Chef
(Name/Title/Phone Number!E-mail) (910) d- fy)n.register.civ@mail.mil

FILE LOCATION:

SACO's NAME MAJ Angella Beji, Info System Officer
(Name/Title/Phone Number!E-mail) (910) 570-8651, angella.m.beji.mil@mail.mil

RECOMMENDATION FOR STAFF PRINCIPAL:

9. STAFF COORDINATION

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

10. REMARKS: D RETURNED REQUESTING ADDITIONAL INFORMATION/CLARIFICATION

(