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

AFRC-CI 11 Mar 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Reserve Access Control Policy

1. References:

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

b. United States Army Chief Information Officer (CIO)/G-6 Cyber Directorate Information Assurance Best Business Practice (IA BBP) 04-IA-0-0001, Army Password Standards, Version 2.5, 1 May 2008.

c. 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).

d. JTF-GNO CTO 07-015, Public Key Infrastructure (PKI) Implementation, Phase 2, 11 December 2007.

e. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, Revision 1, 10 June 2014.

f. Department of Defense (DoD) 8570.1M, Information Assurance Workforce Improvement Program, Change 4, 10 November 2015.

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

h. United States Army Reserve Command (USARC) CIO/G-6 Access Control Standard Operating Procedure (SOP), https://xtranet/usarc/g6/ITG/SitePages/IT%20Governance.aspx.

2. Purpose: The purpose of this policy is to establish guidance for the effective implementation of Risk Management Framework (RMF) security controls and control enhancements in the Access Control (AC) family. This policy reflects management

commitment and applicable federal laws, directives, regulations, and guidance. This policy is intended for unrestricted electronic dissemination to all USAR units serviced by the USARC CIO/G-6.Cybersecurity Operations Branch (COB) via SharePoint.

3. Applicability: This policy applies to all users and potential users of supported information systems connected to all USAR managed networks (unclassified and classified) directly, wireless or through remote connections, stand-alone clients, and servers. This policy also applies to organizational units, and controlled information systems and their users and System/Network Administrators (SA/NAs).

4. Policy:

a. In accordance with reference 1e, all RMF controls within the AC family will be met to satisfy the security requirements and to adequately mitigate the risk incurred by using information and information systems in the execution of organizational and business functions. This document will also satisfy the requirements of the Department of the Army Inspector General (DAIG).

b. USAR will ensure that the most basic security requirements are not only met, but that all users take a proactive role in the protection and accessibility of their data and assets.

c. Compliance with RMF access controls will be monitored on an ongoing basis by USARC CIO/G-6 COB and Cybersecurity Program Management Division personnel who will provide guidance on managing information security risk at three distinct tiers-organization level, mission/business process level, and information system level.

d. ISE is the port security for the network and utilizes 802.1x. If a device is not compatible with 802.1x, a bypass process has been engineered to maintain the operation of the end device without compromising security.

5. Responsibilities:

a. USARC CIO/G-6 Organizational Responsibilities:

(1) Cybersecurity Operations Branch (COB) will perform all cybersecurity-related functions included within this policy. The COB will perform continuous compliance auditing for all related cybersecurity functions and report results to USARC CIO/G-6.

(2) Business and Plans Branch will negotiate all service level agreements (SLA), memorandums of agreement (MOAs), and any other contractual documentation related to cybersecurity functions.

(3) Network and Infrastructure, Data Systems and Applications, and Customer Support branches will provide technical expertise to the COB in executing cybersecurity functions. The aforementioned branches must secure all fielded systems in accordance with guidance contained within this policy.

b. Individual Responsibilities:

(1) Directors/Commanders will:

(a) Sign appointment orders that define a user's role (e.g., SA/NAs) employing least privilege for specific duties and information systems, ensuring that the processes operate at privileged levels no higher than necessary to accomplish the required mission/business functions.

(b) Ensure RMF and NIST SP 800-53A controls within the AC family are followed in accordance with this policy, DoD Instructions (DoDIs), DoD Directives (DoDDs), other SPs, and Army regulations.

(c) Enforce local command in-processing/out-processing SOPs to ensure accounts are created/removed/deleted/transferred as user status changes.

(d) Appoint in writing Trusted Agents (TAs) or Enhanced Trusted Agents (ETAs) using an approved CIO/G-6 memorandum template.

(e) Authorize Active Directory privileged-level access. Verify registration, training requirements, and documentation/certifications have been uploaded to the Army Training and Certification Tracking System (ATCTS).

(2) Information System Security Manager (ISSM) will:

(a) Act as the COB Chief.

(b) Develop Cybersecurity SOP that ensures organizational compliance to this policy.

(c) Sign Privileged Access Agreements (PAAs).

(d) Verify the subscriber DD Form 2842s (DoD Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities) are updated and signed annually.

(e) Unit commander will sign appointment orders that define a user's role (e.g., SA/NAs). Ensure access controls are followed in accordance with this policy, DoDIs, DoDDs, SPs, and Army regulations.

(f) Appoint in writing Trusted Agents (TAs) or Enhanced Trusted Agents (ETAs) using an approved CIO/G-6 memorandum template.

(g) Authorize Active Directory privileged-level access. The USARC Organizational Information System Security Manager (ISSM) has final approval for all administrators.

(h) Audit, review, and revalidate privileged network accounts on a continuous 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.

(i) Approve or decline devices being added to the MAC Authentication Bypass Database.

(3) Privileged Users: SA/NAs, Computer Programmers, and Workstation Administrators will:

(a) Be appointed by their Mission Support Command commander, staff principle, tenant, director, or camp/post/station.

(b) Be issued official appointment orders assigning personnel to IAT-11 or higher positions, which must be uploaded to their ATCTS profile, and complete the mandatory Cyber Security Fundamentals training (https://ia.signal.army.mil/IAF/default.asp).

(c) Complete PAAs, which must be approved by the COB ISSM prior to the users uploading them to their ATCTS profiles. Privileged users must sign and upload PAAs to ATCTS annually.

(d) Upload all valid commercial certifications. Baseline certification must be current (not expired) and/or Information Assurance (IA) personnel must be enrolled in Continuing Education as outlined by the vendor. Computing Environment

Certification/Training will be determined by the direct Government Supervisor. Refer to DoD 8570.1M for further guidance.

(e) Login with their Non-Secure Internet Protocol Router (NIPR) Alternate Smart Card Logon (ASCL) on network or virtual private network (VPN), or Secure Internet Protocol Router (SIPR) ASCL. Administrators are required to use their regular Common Access Cards (CACs) for non-privileged functions. SA/NAs are authorized to use privileged commands via remote access when mission requirements arise, i.e. maintenance.

(f) Use automated tools in Active Directory for account management.

(g) Administrators who manage Active Directory privileges will run queries for stale/inactive accounts that have not been accessed for 45 or more days. Accounts determined to be inactive for 90 or more days will be disabled and a notice will be sent to the users.

(h) Computer Programmers will only execute software applications/programs with elevated privileges to perform required functions. Code will not be executed at a higher level than the privileges assigned to organizational users/programmers.

(i) Conduct required Defense Information System Agency Security Technical Implementation Guide (STIG) scans quarterly and upload findings and mitigations to Enterprise Mission Assurance Support Service (eMASS) as required.

(j) Register to receive Army Information Assurance Vulnerability Management notices. To register, send an email to army.iavm@us.army.mil with "Subscribe" in the Subject line and System Administrator Army Knowledge Online (AKO) username in the message body.

(k) Ensure all required security programs, including, but not limited to: Endpoint Security (i.e., Host Based Security System) modules, current anti-virus program, and definition files, are installed.

(l) Review information system and network audit logs and log files daily, and report anomalies or suspicious information in accordance with installation incident response reporting. Maintain audit logs for 1 year.

(m) Monitor information system performance to ensure that recovery processes, security features, and procedures are properly restored after an information

system or critical service failure has been restored or has been rebooted, which is required annually per the Army Portfolio Management Solution (APMS).

(n) Monitor information system performance to ensure that processes, security features, and operating system configurations are not altered. Ensure applicable Standard Consent Banner and User Agreements are applied through group policy objects and/or the Army Gold Master (AGM) baseline images to computers, websites, and applications.

(o) Complete PAAs, which must be approved by the COB ISSM prior to the users uploading them to their ATCTS profiles. Privileged users must sign and upload PAAs to ATCTS annually.

(p) Upload all valid commercial certifications. Baseline certification must be current (not expired) and/or Information Assurance (IA) personnel must be enrolled in Continuing Education as outlined by the vendor. Computing Environment Certification/Training will be determined by the direct Government Supervisor. Refer to DoD 8570.1M for further guidance.

(q) Login with their NIPR ASCL or SIPR ASCL to perform elevated privilege functions on information systems. Administrators are required to use their regular CACs for non-privileged functions.

(4) Security Officers will:

(a) Establish a clear need-to-know for prospective recipients; ensure issuance of a proper clearance and signed Classified Information Non-Disclosure Agreement prior to granting access to classified information and information systems.

(b) Take the proper precautions to ensure that unauthorized persons do not gain access to classified information and that classified information, systems, and media are properly protected, controlled, marked/labeled, and stored at the appropriate classification level and will not be made publically accessible.

(c) Ensure all SF 701's End of Day Checks, SF 702 Security Container Checklist and DA Form 1999 Visitor Log

(d) Transmit classified information through approved channels by the most secure and expeditious method.

(5) Contracting Officer Representatives (CORs) will:

(a) Create, manage, and maintain access control list and rosters. Authorization will be obtained from senior leadership prior to being posted for compliance.

(b) Create, manage, and maintain access control list and rosters. Authorization will be obtained from senior leadership prior to being posted for compliance.

(c) Access control for physical environment, network accounts, and related security access concerns will be managed and tracked thought the use of applicable list and rosters.

(6) All users will:

(a) Complete a DD Form 2875 (System Authorization Access Request) before establishing a wired, wireless, or VPN connection.

(b) Complete the DoD Cyber Awareness Challenge Training (https://ia.signal.army.mil/DoDIAA/default.asp). The DoD Cyber Awareness Challenge Training and exam is an annual requirement and must be completed annually to maintain access to USAR managed networks.

(c) Register for and/or update the ATCTS account at https://ate.us.army.mil/iastar/index.php.

(d) Read, sign, and upload the AUP and DD Form 2875 to ATCTS and/or retain a copy for their records. The AUP will be signed and uploaded to ATCTS prior to accessing the network (local or remotely) annually.

(e) Access information systems using Government owned/authorized devices connecting directly to the network, wireless or VPN, using CAC user based enforcement. Remote access is available via VPN or wireless and is approved for use when mission/operational requirements arise.

(f) Log off their computer at the end of the duty day or whenever they expect to be away from their computer for an.extended period of time during the duty day. User local, network, and remote access sessions will be automatically terminated after 60 minutes of inactivity.

(g) Responsible for marking and labeling of electronic media or other means to reflect the highest classification of information it contains (e.g., For Official Use Only (FOLIO), or Personally Identifiable Information (PII)).

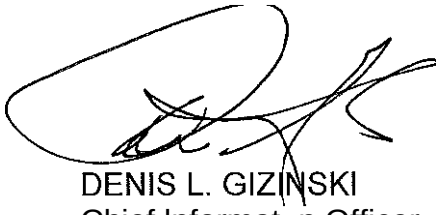
(h) Safeguard information related to national security systems and PII that they have access to and will follow the requirements of this policy and other applicable regulations, directives, and policies. Any PII that is stored on any USAR hosted application may be accessed and/or amended using only that application.

(i) Not use personally owned devices and/or information systems on a Government network; connecting these devices is prohibited. Only use information systems or approved storage devices that are configured and authorized to store PII (e.g., data-at-rest solution and/or encryption mechanisms.)

(7) Guest accounts: USARC permits users to log onto USAR managed network assets on a guest account with limited access to network functionality to complete training requirements necessary to meet DoD 8570 training requirements. These accounts are for USAR personnel only and will expire 6 days after creation. Guest accounts are only authorized for use of cleared USAR visitors while in-processing.

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. GIZINSKI
Chief Informat n Officer
USARC Deputy Chief of Staff, G-6

DISTRIBUTION:

GEOGRAPHIC COMMANDS:
1 MSC
7MSC
9 MSC
63 DIV (R)
- USAG-FHL
81 DIV (R)
- USAG-Fort Buchanan
(CONT)

DISTRIBUTION: (CONT)
88 DIV (R)
- USAG-Fort McCoy
99 DIV (R)
-ASA-Dix

FUNCTIONAL COMMANDS:
3 MCDS
760RC
79TSC
200 MP CMD
311 SC(T)
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
(CONT)

DISTRIBUTION: (CONT)
8THARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
lll CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

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

)

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)* 20171106	3. SUSPENSE DATE *(YYYYMMDD)* 20171110
4. OFFICE SYMBOL	5. SUBJECT United States Army Reserve Access Control Policy		

6. ROUTING:	**Initial**	**Date**	POC *(Rank,-Naffle,-P_hone)* **DIR**
			COMMENTS:

7. EXECUTIVE SUMMARY/ ACTION MEMORANDUM

Key Points

- This policy reflects management commitment and applicable federal laws, directives, regulations, and guidance.
- This policy is intended for unrestricted electronic dissemination to all USAR units serviced by the USARC CIO/ G-6 Cybersecurity Operations Branch (COB) via SharePoint.
- This policy applies to all users and potential users of supported information systems connected to all USAR managed networks directly, wireless or through remote connections, stand-alone clients, and servers.

Ref:

Encl: TAB A: CIO/G6 Form 5 Routing Sheet
TAB B: United States Army Reserve Access Control Policy

1. Purpose:

The purpose of this policy is to establish guidance for the effective implementation of Risk Management Framework (RMF) security controls and control enhancements in the Access Control (AC) family.

2. Discussion:

In accordance with reference 1e, all RMF controls within the AC family will be met to satisfy the security requirements and to adequately mitigate the risk incurred by using information and information systems in the execution of organizational and business functions. This document will also satisfy the requirements of the Department of the Army Inspector General (DAIG).

USAR will ensure that the most basic security requirements are not only met, but that all users take a proactive role in the protection and accessibility of their data and assets.

Compliance with RMF access controls will be monitored on an ongoing basis by USARC CIO/G-6 COB and Cybersecurity Program Management Division personnel who will provide guidance on managing information security risk at three distinct tiers-organization level, mission/business process level, and information system level.

ISE is the port security for the network and utilizes 802.1x. If a device is not compatible with 802.1x, a bypass process has been engineered to maintain the operation of the end device without compromising security.

3. Recommendation:

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

8. LEAD AGENCY STAFF COORDINATION | TRACKING NUMBER:

TITLE	INITIAL	TYPE OR PRINT NAME	
Deputy		Mr. Denis, Gizinski	
PRINCIPAL			

ACTION OFFICER *(Name/Title/Phone Number/E-mail/-)*	Mrs. Kimberly Register, CPMD Chef (1D 51a; s'!r{k;:;;6'erly.m.register.civ@mail.mil	
FILE LOCATION:		
SACO'sNAME *(Name/Title/Phone Number!E-mail)*	MAJ Angella Beji, Info System Officer (91O) 570-8651, angella.m.beji.mil@mail.mil	

RECOMMENDATION FOR STAFF PRINCIPAL:

9. STAFF COORDINATION

CONCU	NON-CONCUR	AGENCY	NAME *(TITLE, LAST NAME)*	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					
D	D					

10. REMARKS: D RETURNED FI QUESTING ADDITIONAL INFORMATION/CLARIFICATION