NATIONAL GUARD BUREAU
111 SOUTH GEORGE MASON DRIVE
ARLINGTON VA 22204-1382

ARNG-HRP 24 April 2023

MEMORANDUM FOR G1s of All States, Puerto Rico, Guam, Virgin Islands and District of Columbia (hereinafter referred to as “States”)

SUBJECT: State Interactive Personnel Electronic Records Management System (iPERMS) Domain Management Guidance (PPOM 23-007)

1. References:

a. Army Regulation (AR) 600-8-104, Army Military Human Resource Records Management.

b. Department of the Army Pamphlet (DA PAM) 600-8-104, Army Military Human Resource Record Management.

c. System Authorization Access Request with Favorable Background Investigation Required to Access Personnel Systems in the Army National Guard (ARNG) Human Resource (HR) Domain, Personnel Policy Operational Message (PPOM 18-040).

d. State Interactive Personnel Electronic Records Management System (iPERMS Domain Management Guidance.

2. Purpose. This memorandum implements responsibilities, guidance, and procedures for iPERMS management at the National Guard Bureau level and below.

3. Responsibilities.

a. Personnel Actions Branch ARNG-HRP-R, iPERMS Section will:

(1) Perform system administration of entire National Guard (NG) domain.

(2) Provide the State iPERMS Domain Managers (DMs) with tools, training, resources, systems, and programs to execute core human resource (HR) activities.

(3) Maintain oversight over all DMs, periodic state system-wide audit reports, grant and remove iPERMS permissions as needed in concert with the appropriate State DMs, and communicate changes and updates to the G1 community

(4) Conduct periodic review/audit(s) of State DMs actions to ensure they function in accordance with established rules, regulations, and guidelines.

(5) Coordinate with Human Resources Command on NG mission requirements and provide the Command (NGB) with all updated HR issues.

(6) Identify documents that should be added to or removed from iPERMs by recommending updates to AR 600-8-104.

(7) Approve all iPERMs related exceptions to policy.

b. The State G1 will:

(1) Appoint no more than two DMs to iPERMS per State/Territory. A third DM may be appointed to facilitate State needs. Submit request to the Personnel Actions Branch ARNG-HRP-R, iPERMS Section.

(2) Appoint DMs in the rank of SFC or higher; or a GS-09 and above.

(3) Ensure DMs conduct periodic audits of iPERMS users and activities within their State domain.

(4) Ensure State DMs and DAs with user and document management permissions attend training IAW paragraph 4d.

(5) Verify that all DMs and DAs have a current security clearance, per PPOM 18-040, paragraph 4 prior to granting access.

c. State Domain Manager will:

(1) Conduct custodial records oversight and actions for their State, to include the creation, protection, and maintenance on the Army Military Human Resource Record (AMHRR) for Soldiers within the domain in accordance with all federal laws, state statutes, DoD and Army regulatory guidelines.

(2) Roles. DMs have the authority to assign, remove and unlock user accounts for all available roles and rules. DMs will have oversight of subordinate users with elevated rules and roles.

d. Domain Administrators will manage users within their hierarchy based on the rules and options assigned by the State DM. The DA must have an Authorized Official (AO) Rule assigned.

e. Problem Resolver (PR) will resolve all problems cases in a timely manner.

f. Quality Control (QC) personnel will manage and work all input queues.

g. Verifiers (VR) will verify or substantiate documents indexed and verified by the Index/Validation user.

h. Index/Validation (IV) users will index and validate all scanned or uploaded documents.

i. Scan Operators (SO) will scan or web upload documents.

j. Field Operators (FO) will scan documents to be automatically routed to the Soldier's domain.

k. Authorized Officials (AO) will receive "view only" permissions to documents pertaining to one or more Soldiers based on a confirmed need-to-know when a DM or DA applies an Authorization Rule.

l. Records Managers (RM) will conduct a Personnel Record Review (PRR) of Soldiers' records, no less than annually IAW AR 600-8-104.

4. Guidance and Procedures.

a. Access requirements for all users; Personal Identifiable Information (PII) (https://cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/), annual Cyber Awareness Training (https://cs.signal.army.mil/UserMngmt/UserPortal.asp) and iPERMS Web Based Training (WBT) for roles requested (https://ipermstraining.carson.army.mil/wbt/index.jsp).

b. Verify that all end users have a favorably completed National Agency Check (NAC)/background check or hold a clearance, per PPOM 18-040, paragraph 4 prior to granting access.

c. Accounts must be activated within 30 days of creation by logging into iPERMS and using the assigned rule. All users must log into a role assigned and perform functions no less than every 90 days to prevent system revocation of all roles.

d. DM/DA training requirements. After appointment and prior to assuming DM or DA responsibilities, a DM/DA must attend the Administrative Phase 1 and Phase 2 training. DM/DA will attend this training every two years to stay current with functional procedures and reports. If training dates are unavailable, an exception to policy may be requested from ARNG-HRP-R.

e. The DM will ensure that all users, other than Soldier viewing their own records, have completed the WBT module(s) that correspond to their assigned role(s). There is no annual requirement for recertification.

f. DMs must utilize AR 600-8-104 and DA PAM 600-8-104 for policy and clarification.

g. PRs must resolve/verify the PR cases in a timely manner due to the negative effects PR cases have on promotions, record reviews, educational opportunities, and other personnel actions. PR cases should be checked by DODID# or SSN prior to any selection/ promotion board proceedings.

h. Release of restricted data. All documents in the Restricted Folder should have filing instructions i.e., regulatory guidelines, Department of Army Suitability Evaluation Board (DASEB) or Army Board Correction of Military Record (ABCMR) memorandum directing documents into the Restricted Folder. This includes Soldiers who have changed their status (from Enlisted to Officer or Officer to Enlisted) as stated in AR 600-8-104, Paragraph 3-10. While no access request to a personnel record will be denied as long as the user has a need-to-know, no requester/ organization will be granted access to the whole OMPF (including the Restricted Folder) unless the request is in writing and on a case-by-case basis. Selection Boards and Career Counselors/ Managers should not be reviewing the Restricted Folder per AR 600-8-104 Table 3-1.

i. Requests to access Soldier’s records by investigative offices

(1) Staff Judge Advocate record requests. AMHRR requests must be on the requesting Staff Judge Advocate unit's letterhead and include the Soldier's /DODID #, Name, Rank, reason for request, the trial counsel's name, email address and phone number.

(2) 15-6 Investigating Officers. AMHRR Requests must include the investigator's name, email address, phone number, reason for request, a copy of their appointment orders and the Soldier's DODID #, Name, Rank.

j. System Audits. DM will conduct monthly system audits of authorized users, create, revise or remove access rules deemed to be outdated, illegal, or inadequate and remove access permissions from those who no longer require elevated access to the system.

k. DD 93/SGLV 8286 Audit. DMs will ensure DAs and RMs are accurately monitoring unit readiness of DD 93 and SGLV 8286 IAW AR 600-8-1.

l. Document Removal. Documents will not be removed from iPERMS without just cause or regulatory guidance. Once scanned in to iPERMS, a document becomes a permanent part of the AMHRR. The document will not be removed from the iPERMS database or moved to another part of iPERMS unless directed by the following:

(1) The Army Board of Correction of Military Records

(2) The Department of the Army Suitability Evaluation Board

(3) Army Appeal Boards

(4) Chief, Appeals and Corrections Branch

(5) The State DM or DA when documents are duplicates or have been improperly filed. These documents should be removed using the Problem Resolver Tool.

m. Enforce personnel record integrity by ensuring no Soldier processes their own individual documents into their iPERMS record. It is unethical and breaks the 'chain of custody', it opens the door for fraud and provides unfair advantage against fellow Soldiers who are not afforded this opportunity. .

n. Direct all suspected cases of fraud to the appropriate 15-6 investigation appointing authority for further action. If an investigation is opened, suspend the user's access and flag them to prevent favorable personnel actions. Use flag code L – Commander's Investigation.

5. The points of contact for this memorandum are Timothy Taylor at CML 703-607-7512 or by email at timothy.taylor5.civ@army.mil. and Reggie Alexander at CML 703-604-8216, or by email at reggie.l.alexander.civ@army.mil.

SKELTONRILEY.HEIDI.MAE.1239039568

Digitally signed by SKELTONRILEY.HEIDI.MAE.1239039568
Date: 2023.04.24 16:27:35 -04'00'

HEIDI M. SKELTON-RILEY
COL, AG
Chief, Personnel Division