Interactive Personnel Electronic Records Management System (iPERMS)

Standard Operating Procedures (SOP)

NGRI-MPO-PSB
NOVEMBER 2024

UNCLASSIFIED

Chapter 1
General Information

1-1. Purpose
To establish procedures for the Rhode Island Army National Guard (RIARNG) Records Custodians at all levels and provide guidance to create, handle, and properly maintain the personnel record electronic workflow process within iPERMS.

1-2. References
See Appendix A.

1-3. Scope
All personnel processing administrative functions in the RIARNG will adhere to the procedures in this SOP and all Army regulatory policies, Army directives and procedures. The RIARNG iPERMS SOP encompasses administrative operations, records management and recurring tasks that are standardized and routine.

Chapter 2
Safeguarding Records and Security

2-1. Safeguards
Title 44 U.S. Code chapter 31. 3105. states that the head of each Federal agency shall establish safeguards against the removal or loss of records, the head of such agency determines to be necessary and required by regulations of the Archivist. Safeguards shall include making it known to officials and employees of the agency that records in custody are not to be alienated or destroyed except in accordance with sections 3301–3314 of this title, and the penalties provided by law for the unlawful removal or destruction of records.

2-2 Unlawful Removal or Destruction of Records
Title 44 U.S. Code chapter 31. 3106. States that the head of each Federal agency shall notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the agency, and with the assistance of the Archivist shall initiate action through the Attorney General for the recovery of records the head of the Federal agency knows or has reason to believe have been unlawfully removed from that agency, or from another Federal agency whose records have been transferred to the legal custody of that Federal agency.

In any case in which the head of a Federal agency does not initiate an action for such recovery or other redress within a reasonable period of time after being notified of any such unlawful action described in subsection (a), or is participating in, or believed to be participating in any such unlawful action, the Archivist shall request the Attorney General to initiate such an action, and shall notify the Congress when such a request has been made.

2-3 Concealment, Removal, or Mutilation of Records
Fraud and forgery potentially occur at every level of all ranks. It degrades the integrity of Army systems and should be taken seriously. Fraud and forgery must be reported immediately.

Failure to comply with Federal law and records management guidelines prohibiting unauthorized removal, mutilation, destruction, or falsification of documents is punishable under title 18 U.S. Code Part I chapter 101.

2-4. Release of Information and Privacy Act
All request(s) of records for active and inactive soldiers of the RIARNG from an outside agency and/or civilian agencies will be directed to the Personnel Service Branch (NGRI-MPO-PSB). The Standard Form 180, Request Pertaining to Military Records is used to request information from military records. The request will be signed by the soldier and the signature will be verified with a source document for authentication. The Freedom of Information Act, FOIA requests are handled in accordance with AR 600-8-104, 2-11.

Special inquiries from investigating officers requesting copies of or access to a Soldier's record, Judge Advocates, inspector general officers, and AR 15–6 investigating officers will submit a written request to the RIARNG iPERMS Domain Manager. At a minimum, requests will include justification, Soldier's first and last name, and complete SSN. AR 15–6 investigating officers will also include appointment orders.

Record Custodians and authorized officials will use the Army Privacy and Civil Liberties Program, AR 25-22, to safeguard the right to privacy and handle personally identifiable information of active and inactive soldiers. No person is entitled to obtain information from or possess an Official Military Personnel File (OMPF) solely by virtue of his or her position. The OMPF contains privileged materials and will be made available to authorized personnel when required in the performance of official business.
All OMPFs are FOR OFFICIAL USE ONLY unless they are classified higher under the Army Information Security Program, AR 380-5. Classified OMPFs must and will be protected to prevent unauthorized access or disclosure.

2-5. Audit Request
All actions in iPERMs are recorded and tracked. An audit report may be requested through the S1 channel to the state DM utilizing the Memorandum for Record format for explicit deletion of documents without justification; misuse of viewing documents or records without a need to know; iPERM clerk failure to submit and complete documents; violation of the Privacy Act of 1974 and various investigations as needed.

Chapter 3
Requirements and Access Request

3-1. Access to iPERMS
All active and inactive Soldiers' information and records contained in iPERMs are governed by the Privacy Act of 1974 and AR 25-22. The Privacy Act Statement in figure 2-1 of AR 600-8-104 identifies the information that will be used to verify an authorized official and information used to manage Soldier records in iPERMs and iPERMS-S.

3-2. Access Request
Access to a Soldier's individual record in iPERMS is automatic upon accession. All personnel authorized to perform routine records maintenance, process personnel actions, perform other personnel management functions, or with an official need to know information from a RIARNG Soldier's iPERMs record will request iPERMS access using the DD Form 2875, System Authorization Access Request (SAAR).

The DD form 2875 must be signed by a military supervisor in the grade of sergeant first class or above. Civilian supervisors must be a general schedule (GS)-11 equivalent or above. Requests for access to the restricted folder must be signed by a colonel or GS–14. Access requests are approved at the state level. The DD form 2875 submitted to the NGRI-MPO-PSB will include the completed online Web Based Training (WBT) for the requested role, https://ipermstraining.carson.army.mil/wbt/; current cyber awareness training certificate and personally identifiable information (PII) certificate. The DD 2875 security section must be completed, signed and dated by a security manager.

3-3. Access Revocation
All functions or actions in iPERMS are tracked by audit logs and can be made available with an official request. Users may lose access when PII is not used in accordance with Army regulatory policies, Army directives, and procedures. Access will be revoked for viewing or downloading a Soldier's Army Military Human Resource Record without a mission requirement and/or misuse occurs.

Failure to comply with the guidelines of this SOP and/or Army regulatory policies, Army directives and procedures will result in immediate iPERMS access revocation by the Domain Manager. The revocation notification is sent to the user, supervisor, and Domain Administrator. iPERMs access will be revoked upon ETS, IST, outdated or removal of security clearances and lack of iPERMs access for 30 days or more.

3-4. Network
All document submissions, batches, reports, and Soldier document reviews will take place over a secure network. Network: https://iperms.hrc.army.mil/rms.login.jsp. All users will have and use their own iPERMS account when accessing iPERMS.

Chapter 4
Roles, Rules and Duties

4-1. Domain Manager (DM)
The RIARNG Domain Manager conducts custodial records oversight and actions for the state to include creation, protection and maintenance of the Army Military Human Resource Record (AMHRR) IAW all federal laws, state statutes, DoD and Army regulatory guidelines. The RIARNG DM(s) have the authority to assign, remove and unlock user accounts for all available roles and rules and the oversight of subordinate users with elevated rules and roles. They manage user accounts, access roles/rules and the status of the domain and its workflow. Quarterly system audit of authorized users will be performed at this level. Problem cases are managed at the DM level as applicable and ensure users are resolving cases.

4-2. Domain Administrator (DA)
The RIARNG Brigade elements are allotted two Domain Administrators. The DAs will attend the required DM/DA Administrative Phase 1 and Phase 2 training as directed by State IPERMS Domain Management Guidance PPOM 23-007. They will provide training and oversight to all subordinate personnel as applicable. They will ensure documents are filed IAW AR 600-8-104. Verify all batches from subordinate units and the authenticity of documents within the batches. The DA must ensure all batches in their hierarchy are processed within 60 days of creation. The DA will email a report each month for batches over 60 days. All BDE DAs will manage problem case type 1 and 990 at their level and request DM assistance when necessary. All other problem case types will be processed by the DM(s). **It is the DA responsibility to ensure all required iPPSA input/transaction is complete before pushing records into Soldiers' OMPF.**

4-3. Roles
a. *Index Quality Control (IQC)* is the input side of iPERMS where documents are loaded into the system. The IQC roles are Quality Control (QC), Verifier (VR), and Index/Validation (IV).

b. *Quality Control (QC) (G-1 and BDE)*
The Quality Control role allows the operator to view and process batches grouped in their individual workflow queues, including Index/Validation, Verification, Quality Control, Rescans, Release in Progress, and Input Pending. The QC Operator will not scan documents from this role, as it is not traceable to iPERMS. If the operator scans a document(s) at this level, the same operator cannot be the Verifier or final out in QC. The QC operators are responsible to check for errors that have reached their level. If an error is discovered, or a document is incomplete at the Verifier level, they must assign the batch to the Records Custodian who need to make the necessary corrections.

c. *Verifier (VR) (G-1 and BDE)*
The Verifier role allows the Records Custodian to view batches that have been indexed in the Records Custodian's organization. The Verifier will check all documents for errors by

verifying that the data entered during the Index/Validation is accurate. The VR will compare the data entered by the Index Operator with the data on the document image. They will also check the documents to determine if the correct pages have been joined together and properly named. If an error is discovered at the VR level, return the batch to the IV level Records Custodian to make the necessary corrections. Enter the corrections needed in the comments before returning the document/batch. If the Records Custodian cannot return the batch, it will be routed to the QC level with the comment “Return to batch originator” along with the original correction comments. If the error cannot be corrected and the document need to be reworked and re-scanned, label “Delete” in the comments field with explanation and process to the DA or State level for deletion.

d. *Index/Validation (IV) (All Levels)*

The Index/Validation role allows the Records Custodian to view images of the scanned documents and enter data from those documents into iPERMS. To ensure quality control, all authorized documents per the Document matrix are completed correctly filled out and accurate. Batches will be created in the Index role. Appropriate remarks will be made in the Container, Name, and Comment Fields based on the batch labeling and processing. Images are checked for quality and orientation, and data from those documents is entered into iPERMS. The index data that is entered enables iPERMS users to retrieve all or part of the Soldier’s record. Successful retrieval depends on the accuracy of the information entered and validated during this process. To properly index the documents, you must start by organizing the images in the correct page order if there are multiple page documents. It is necessary for a batch to be finished in the index role before it can move into the batch workflow. Any documents in the batch that are unacceptable, can be rejected and sent to the Rescan module to be corrected, or to Quality Control to be deleted.

e. *Authorized Officials (AO) (All Levels)*

The Authorized Official role provides “view only” access to a record. Access rules will be assigned by the DM. Rules are cumulative, and if more than one rule is assigned, an AO can choose to view records based on a single rule, or the combination of all rules assigned. Access rules will be assigned to allow an AO(s) to view only documents pertaining to a Soldier, a group of Soldiers, or specific documents for Soldiers at their level on a need-to-know basis. They will not have access to General Officer Records, Health and Dental Folders, Evaluations or the Restricted Folders. Only specific individuals with a need to know will have access to those folders.

f. *Problem Resolver (PR) (G-1 and BDE)*

The Problem Resolver resolves and creates problem cases in iPERMS. Problem cases are created by iPERMS input processing (possible duplicate documents). A case is a system or document issue that must be resolved by an iPERMS PR. Cases are usually created by the system based on problems with index data. Cases created by individual Soldiers who have a problem require closer attention. There are two queues for case management, assigned and unassigned.

g. *Records Manager (RM) (All Levels)*

The Records Manager serves as the Records Manager for all assigned and attached Soldiers' OMPF. Record Managers have access to view their Soldiers' records and document types as well as review and complete personnel record reviews. RMs will not upload their own AMHRR documents. Record reviews are conducted annually, and all updated documents are scanned and indexed in iPERMS. The Record Manager is required to upload missing documents that were identified during the records review. Record managers are responsible for conducting annual Personnel Record Reviews for all Soldiers within their unit. Conducting records review ensures all required documents are filed correctly in the Soldier record IAW AR 600-8-104 filing requirements and verified. The Record Review validates entries on the record brief, entitlements on the end of month LES, and ensures all substantiating and supporting documents are in the Soldiers' record.

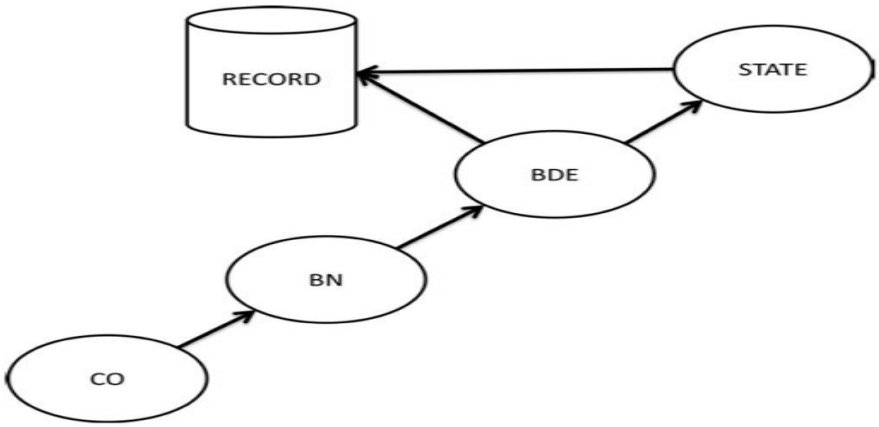
Chapter 5
iPERMs Batch and Responsibility

5-1 Processing Timeline

All batches are processed in a timely manner at all levels. Returned batches must be corrected and actioned no later than 60 days. The DAs must ensure all batches in their hierarchy are processed within 60 days of creation. The DM will monitor stagnated batches at all levels. During an absence, such as leave or schools, at any level, ensure there is coverage from the same level or the next level higher within the Unit, Battalion, Brigade or G1/State. The absent user will inform the secondary user at their level, designated DA or DM at the Brigade or G1/State level, to ensure batches will bypass the vacant level and continue to process.

5-2 Batch Workflow

The workflow is the process of batches moving from one point to another. This may be at the same level or up the hierarchy. iPERMS uses the hierarchy as defined by IPPSA. Unit IV will conduct the initial upload of most documents and send to the next level. Batches should flow from the lowest level to the highest. Regardless of level, unit, battalion, brigade or state, **the batch will have a minimum of two different users reviewing the batch before it's pushed into the Soldiers' record.**



5-3 Rejecting Documents

Indexers, Verifiers, and Quality Control Operators can reject an image or document for several reasons. Entire batches can be rejected and sent to the Quality Control queue. Batches can also be split, sending the rejected documents to a new batch, while the remainder of the batch moves through input processing. This allows the Records Custodian time to work on the rejected documents in the split batch without delaying the processing of the remainder of the original batch. A Records Custodian can assign a "Reject Code" for each rejected document. The Reject Code determines where the rejected document will go when the batch is split. Rejected documents may go to Index/Validation or Quality Control.

5-4 Responsibilities

a. *Company/unit administrator(s)* is responsible for scanning and indexing all documents at the unit level. Track batches in the workflow, ensuring accuracy, validity and completion. Serves as the Records Manager for all assigned and attached Soldier's iPERMs, except for RSP Soldiers. Ensure all documents in a Soldier's AMHRR belong to that Soldier and are properly indexed into the correct record. All iPERMs documents have the correct name, effective date and free of alterations and/or falsified information. **RMs are not authorized to release records to third parties.** All batches are actioned within the allotted timeframe, documents returned for corrections are actioned and processed accordingly. **All required IPPSA transactions are completed before batch submission to the next level.**

b. *Battalion administrator(s)* is responsible for verifying all batches internally and from subordinate units, ensuring accuracy and validity. Track all batches in the workflow, ensuring accuracy and completion. Track rejected documents and batches ensuring corrected actions are completed and documents processed into Soldier records. **All required IPPSA transactions are completed and verified before batch submission to the next level.**

c. *Brigade administrator(s)* is responsible for verifying all batches internally and from subordinate battalions/units, ensuring accuracy and validity. Ensure subordinate units and battalions are completing all required iPERMs and IPPSA transactions. Assist RM manage and track annual Soldier record reviews. Track rejected documents and batches, ensuring appropriate action and the completion of the documents and batches. Removal, mutilation, destruction and falsification are prohibited per regulatory and federal guidelines. Ensure all subordinate units and battalions are submitting documents appropriately and IAW AR 600-8-104. **At this level, it is imperative that all required IPPSA transactions are verified and actioned. Ensure quality assurance is completed to identify discrepancies and errors before documents are processed to Soldiers' records.**

d. *Personnel Service Branch (PSB)* is responsible for assisting all subordinate elements upon request and/or as applicable. Scan and index all iPERMs authorized documents IAW AR 600-8-104 when created, finalized and/or acquired. Receive and action all applicable batches per the state iPERMs batch workflow. **Verify and/or input IPPSA transactions when required.**

Appendix A
References

AR 25-2
Army Cybersecurity

AR 25-22
The Army Privacy and Civil Liberties Program

AR 380-5
Army Information Security Program

AR 600-8-104
Army Military Human Resource Records Management

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

DoDI 1336.08
Military Human Resources Records Life Cycle Management

DoDI 5015.02
DoD Records Management Program

PPOM 18-040
System Authorization Access Request with Favorable BI Required to Access Personnel Systems in the National Guard (ARNG) Human Resources (HR) Domain

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

The Privacy Act of 1974 (5 USC 552a)

Title 44, United States Code, Chapters 29
Management by the Archivist of the United States and by the Administrator of General Services

Title 44 United States Code, Chapter 31
Records Management by Federal Agencies

Title 44 United States Code, Chapter 33
Disposal of Records