GAARNG Standard Operating Procedures

Human Resource Systems Branch (NGGA-PES)

Human Resource Systems

Joint Force Headquarters
Georgia Army National Guard
Marietta, GA
1 October 2025

UNCLASSIFIED

Contents

Chapter 1 Introduction
1-1. Purpose
1-2. Applicability
1-3. Privacy Act
1-4. Fraud and Forgery

Chapter 2 Integrated Personnel and Pay System - Army (IPPS-A)
2-1. Overview
2-2. Access
2-3. Roles
2-4. IPPS-A Audits
2-5. Workflow Templates
2-6. S1 Pool
2-7. Responsibilities
2-8. Retirement Points Accounting Management (RPAM)

Chapter 3 Interactive Personnel Electronic Records Management System (iPERMS)
3-1. Overview
3-2. Access
3-3. Roles
3-4. Responsibilities
3-5. Personnel Record Review

Chapter 4 Directors Personnel Readiness Overview (DPRO)
4-1. Overview
4-2. Access
4-3. Functions and Features

Chapter 5 Record Brief
5-1. Overview
5-2. Access
5-3. Roles
5-4. Responsibilities

Chapter 6 GA Power App Catalog
6-1. Overview
6-2. Access
6-3. Applications

Chapter 7 SGLI Online Enrollment System (SOES)
7-1. Overview
7-2. Access
7-3. Responsibilities
7-4. Timeline

Chapter 8 Real-time Automated Personnel Identification System (RAPIDS)
8-1. Overview
8-2. Access
8-3. Roles and Responsibilities

Chapter 9 Interstate Transfer (IST)

9-1. Overview
9-2. Inbound Transfers
9-3. Outbound Transfers
9-4. Responsibilities
9-5. Required Documents
9-6. Procedure

Appendix A References
Section I Publications
Section II Forms
Section III Abbreviations

Appendix B Authority within IPPS-A
Section I Approval Authority within IPPS-A
Section II Subcategory Authority within IPPS-A

Appendix C DD Form 2875 Instruction

Appendix D Managing User Access and Batch Workflow within iPERMS
Section I Assigning User Role(s) and Rule(s)
Section II Batch Workflow

Appendix E RAPIDS Access and Training

Chapter 1
Introduction

1-1. Purpose
This Standard Operating Procedure (SOP) outlines the policies and procedures for Georgia Army National Guard (GAARNG) Soldiers using Human Resource (HR) Systems. It covers accessing, managing, and updating personnel records within those systems.

1-2. Applicability
This SOP applies to all personnel supporting administrative functions within the GAARNG. It standardizes administrative operations and recurring tasks. All personnel will also adhere to applicable Army National Guard and Department of Army directives.

1-3. Privacy Act
a. Personnel managing Army Military Human Resource Records (AMHRR) must comply with the Army Privacy Program to protect the privacy of current and former Soldiers. Access to AMHRR information is based on need-to-know, not solely on position.

b. Before releasing any Soldier's information or documents to individuals or organizations outside the GAARNG or partner agencies, users must obtain signed consent for the release of information from the Soldier. The user must verify the Soldier's signature against another signed document to ensure authentication.

c. All AMHRRs are considered Controlled Unclassified Information (CUI) unless classified higher per AR 380-5. Classified AMHRRs require protection against unauthorized access or disclosure.

1-4. Fraud and Forgery
a. Fraud and forgery are intentional acts to deceive, falsify, or alter official records, signatures, or data for personal gain or to influence official actions. This includes manipulating system data, creating false documents, or misrepresenting information.

b. Fraud and forgery can occur at any level and involve Soldiers of all ranks. These actions compromise the integrity of Army systems and violate Army Values. All HR system users, leaders, and Soldiers must take these offenses seriously. Report suspected fraud or forgery immediately to the HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

c. Confirmed instances of fraud or forgery will result in immediate suspension of system access and appropriate disciplinary action, as determined by the commander or supervisor. The HR Systems Branch will correct affected systems with accurate data.

Chapter 2
Integrated Personnel and Pay System - Army (IPPS-A)

2-1. Overview
IPPS-A is the Army's integrated personnel and pay system. This system combines personnel actions with pay transactions, streamlining HR processes and reducing errors. Soldiers can access and manage their personal information 24/7 through the IPPS-A Self-Service Web Portal.

2-2. Access
All GAARNG Soldiers have automatic basic access to the IPPS-A Self-Service Portal. For access issues, contact the G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil. Requests for elevated access will be processed according to the procedures outlined in this SOP.

a. IPPS-A can be accessed at https://hr.ippsa.army.mil/.

b. Users requiring elevated access in IPPS-A must complete appropriate parts of Distance Learning (DL) courses based on their duty position, and an Instructor Facilitated Training (IFT) hosted by the GAARNG G-1.

(1) Enrollment into DL is self-managed via IPPS-A Self-Service portal, and IFT is managed by G-1 HR Systems Branch. New users can access IPPS-A (URL above) to complete DL, then schedule themselves for an IFT course via Microsoft Teams (Systems channel within GAARNG G1 - see Appendix B.)

(2) Once both DL and IFT are complete, users will log into IPPS-A in order to request elevated user access. Access request may be submitted by the user him/herself, or other HR Professional with elevated user access on user's behalf. When submitting the request, users will provide the following information in the comments block:

(a) Position Title

(b) Requested Permission

(c) IFT Completion Date

c. Users will be granted the appropriate access levels IAW Appendix B of this SOP.

d. Elevated user access accounts will be automatically or manually de-provisioned in the event one of the following occurs. For restoration of elevated user access, a submission of a new access request is required IAW paragraph 2-2a.

(1) Automatic de-provisions occur when

(a) user receives reassignment or transfer (PCA/TER/XFR);

(b) user does not log on for 90 consecutive days;

(c) or user fails to complete access re-validation prior to expiration.

(2) Manual de-provisions occur when

(a) user loses security clearance level required IAW PPOM 18-040;

(b) or user is found to have been in violation of written policies and guidelines as explained in paragraph 2-4.

2-3. Roles
IPPS-A access is controlled through Roles and Permissions. Roles determine what tasks a user can perform, while Permissions determine which Soldiers a user can access. Detailed information on appropriate Role categories, subcategories, and security settings is provided in Appendix B. Users requiring access beyond the basic self-service level must have their Roles and Permissions requested and approved according to the procedures in this SOP.

2-4. IPPS-A Audits
The integrity of Soldier data that drives all personnel and pay actions is paramount. All transactions within the system are logged, and specific behaviors are monitored within the state in order to help prevent fraud and identify individuals with elevated access in IPPS-A who are attempting to abuse the rights afforded to them. G-1 HR Systems Branch will manage consequences for violating written policies (see Section I of Appendix B.) Violations will be maintained for one year, and result in the following actions:

a. User's first violation will result in a notification to the user's MSC S-1 leadership.

b. User's second violation will result in suspension of elevated access until request for restoration of system access is received from the MSC S1. The G1 and MSC S1 will determine when suspended user access will be restored. This decision will be based on the severity of the violation.

c. User's third violation will result in suspension of elevated access, and suspended user will be re-trained quarterly. Furthermore, the G1, MSC Administrative Officers (AOs) and Chief of Staff will discuss the issue and determine future action for the user.

2-5. Workflow Templates
Workflow template allows HR Professionals the ability to maintain the flow of the submitted PAR. Once a workflow template is built, it can be shared for use by other users. MSC and BN S-1 are expected to perform monthly review of these templates in order to maintain current and relevant workflows. Request for assistance with updates or creation will be submitted to G-1 HR Systems Branch via Microsoft Teams (Systems channel within GAARNG G1 - see Appendix B) or email at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

2-6. S1 Pool
All submitted workflow transactions are initially routed to the S1 Pool, a group of HR Professionals at the Battalion level, that is manually set up and maintained. Submit S1 Pool maintenance request to G-1 HR Systems Branch via Microsoft Teams (Systems channel within GAARNG G1 - see Appendix B) or email at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

2-7. Responsibilities
All users will have access to the Self-Service function. The following sections or individuals are responsible for the information or actions listed below.

a. G-1 HR Systems Branch
   (1) manages user access accounts within IPPS-A;
   (2) provides IPPS-A support to users;
   (3) manages all Enter into and Return from Active Duty (E/RAD) transactions;
   (4) and conducts weekly audits IAW Internal Control Compliance Guide.

b. Human Resource Office (HRO)
   (1) manages actions required for Title 32 Active Guard Reserve (AGR) Soldiers;
   (2) and manages actions required for Title 32 Military Technicians.

c. MSC S-1
   (1) processes personnel actions IAW this SOP;
   (2) conducts monthly review of user access accounts, PAR workflow templates, and S1 Pools within the MSC;
   (3) and manages transactions appropriate for MSC and below.

d. Battalion S-1
   (1) processes personnel actions IAW this SOP;
   (2) and monitors and processes all workflow transactions within the S1 Pool.

e. Individual Soldiers
(1) review and update personnel data;
(2) and notify unit's chain of command of any data discrepancies.

2-8. Retirement Points Accounting Management (RPAM)

a. Overview: IPPS-A now serves as the Authoritative Data Source (ADS) for tracking and managing retirement points data for all Soldiers. Reserve Component Automation System (RCAS) is no longer utilized for this function. IPPS-A automatically calculates and updates retirement points for qualifying services, including Inactive Duty Training (IDT), Annual Training (AT), Active Duty for Operational Support (ADOS), and other types of duty IAW AR 140-185 and NGR 680-2.

b. Access: Soldiers and HR Professionals can view and verify retirement-point totals directly within IPPS-A. Elevated access request for this function follows the same approval process outlined in this SOP.

c. Responsibilities: The G-1 HR Systems Branch maintains system integrity and is the only section authorized to make manual overrides within the Retirement Points module. Soldiers will review their points in IPPS-A at least once a year and notify their Battalion S-1 office to ensure points are reconciled in order to maintain accuracy and compliance.

d. Data Corrections: Battalion S-1 offices unable to reconcile errors or requiring a manual entry (e.g., drilling only for retirement points) will submit a Customer Relationship Management (CRM) ticket in IPPS-A to the provider group "NGGA G-1 RPAM Section."

Chapter 3
Interactive Personnel Electronic Records Management System (iPERMS)

3-1. Overview
iPERMS is an integrated imaging system and powerful database that provides electronic personnel records storage, retrieval, and transfer capabilities, and enhances both mobilization and personnel readiness.

3-2. Access
All GAARNG Soldiers will have access to their own iPERMS records. Users who are experiencing technical difficulties accessing their own iPERMS records may contact G-1 HR systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil for resolution. Users may request elevated role(s) and rule(s), if required to perform daily duty of supporting the administrative functions in the Georgia Army National Guard.

a. iPERMS can be accessed at https://iperms.hrc.army.mil/.

b. Requirements for elevated role(s) and rule(s) are as follows:

(1) New users must complete web-based training for role(s) requested. Training is available at https://ipermstraining.carson.army.mil/wbt/app/. This requirement is only for initial provision. Contact designated Domain Administrator (DA) for questions regarding required role(s) for a specific duty position.

(2) Users must complete and submit System Access Authorization Request (SAAR - DD Form 2875) IAW Appendix C of this SOP. This is an annual requirement.

(3) User access will be automatically de-provisioned in the event a user is moved from one unit to another within IPPS-A. Restoration of de-provisioned user access account will require a new DD Form 2875 completed IAW Appendix C.

c. Users at Human Resource Office (HRO), Health Services Section (HSS), or MSC level and below will contact and submit all required items to their designated DA.

d. Users at all other state staff directorate or users who require DA access will contact and submit all required items to G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

e. DAs will only assign user role(s) or rule(s) IAW Appendix D of this SOP. For any and all exception that is not specifically addressed in this SOP (e.g., Scan Operator, Field Operator roles, or Restricted File access) will be submitted to G-1 HR Systems Branch for approval. Determination for approval of such requests will be made on case-by-case basis.

3-3. Roles
There are several roles within iPERMS, and these roles will be granted based on the user's position and requirements to complete their assigned mission. See Appendix D for details.

a. <u>Authorized Official (AO)</u> only has access to view selected records and document types. They will not have access to General Officer Records, Health and Dental Folders, or Restricted Folder.

b. <u>Field Operator (FO)</u> role provides capability for a user to upload document images into the iPERMS system without requiring specific index information other than Soldier's identification. This role is used when uploading a document for a Soldier whose record belongs to a different domain (other component or state). Documents can be uploaded by scanning or uploading the image files.

c. <u>Scan Operator (SO)</u> is a key step in capturing personnel documents. The scanned images are uploaded, and index data may be associated with images to expedite processing so records may be retrieved and managed. Entry of index data is optional and will be re-validated in the next step of the workflow.

d. Index/Validation (IV) operator enters and validates index data associated with the image so that records may be properly retrieved and managed. It is essential that the data entered and validated during this process are accurate. Users may also upload scanned document images using the IV role.

e. Quality Control (QC) operator has the ability to view and process batches grouped in their individual workflow queues, including IV, QC, Rescans, Release in Progress, and Input Pending. Only G-1 HR Systems Branch and MSC S-1 (including JFHQ) users will be granted QC role.

f. Problem Resolver (PR) has the ability to resolve problem cases in iPERMS. Problem cases may be created by AO, RM, PR operators, or DAs and DMs.

g. Domain Administrator (DA) acts as the records manager and manage iPERMS users within their command hierarchy. Only two users per MSC will be granted DA role, typically the MSC HR Tech and their designee.

h. Records Manager (RM) has access to view selected records and document types. RMs also perform personnel records review.

i. Domain Manager (DM) manages problem cases and ensure users are resolving them. DMs perform periodic audits and manage DAs within the domain.

j. Soldier (SD) may view and download their own documents and report problems within his or her record.

3-4. Responsibilities

The following sections or individuals are responsible for the actions listed below.

a. G-1 HR Systems Branch

(1) manages DM and DA access;

(2) and processes all batches that are labeled “RMS Duplicate Document Case Resolution” by re-indexing correctly.

b. MSC S-1

(1) manages users within the MSC IAW Appendix D of this SOP;

(2) verifies and processes all batches from subordinate BNs and units;

(3) processes all batches in the MSC QC role;

(4) and ensures subordinate BNs and units are completing all required iPERMS actions.

c. Battalion S-1

(1) processes all batches in the BN HR Specialists’ designated role(s);

(2) verifies all batches from subordinate units;

(3) ensures proper records management is taking place in all subordinate units;

(4) receives and reviews iPERMS user requests, ensuring completeness prior to forwarding to the MSC S-1;

(5) and forwards all approved requests for access to the MSC DA for action.

d. Unit

(1) scans and indexes all documents into iPERMS;

(2) provides Soldiers with the opportunity to complete annual Personnel Record Review;

(3) and identifies all documents in the Soldier’s AMHRR that do not belong to that Soldier and utilizes “Report a Problem” tool to initiate record correction request.

3-5. Personnel Record Review

Accurate and current AMHRRs are critical for career development and ensuring correct pay and benefits. To maintain AMHRR accuracy, units must conduct an iPERMS Personnel Record Review annually for all assigned Soldiers, as well as upon their initial arrival to the unit. Detailed guidance for completing these reviews is available on page 8 of the document located at: https://www.hrc.army.mil/wcmt-api/sites/default/wcmtfiles/files/22700_0.pdf.

Chapter 4
Directors Personnel Readiness Overview (DPRO)

4-1. Overview
DPRO is a comprehensive information management system providing access to daily-updated metrics for strength management, attrition/retention, accession, and personnel readiness. It integrates data from numerous external sources, enabling custom reporting and analysis.

4-2. Access
DPRO access is granted based on a user's duty position and command hierarchy. To request access:

a. Log into Guard One (formerly known as RCMS-G G-1 Portal) at https://arngg1.ngb.army.mil/.

b. Select the DPRO application.

c. Select "Request Access" and complete the online form. Select the correct hierarchy and role. Do not select hierarchies outside of Georgia, or a role other than "State User" or "State Power User." Incorrect requests will not be processed.

d. Upload a completed DD Form 2875, following the instructions in Appendix C.

4-3. Functions and Features
DPRO offers several key functions for data analysis and reporting. Detailed information is available in the system's user guide. These include:

a. Dashboards are visual, automatically updated representations of key metrics. Users can utilize pre-defined or customized dashboards.

b. Leadership Reports are pre-configured reports providing quick access to commonly used data.

c. Views are organized collections of metrics focused on specific thems.

d. Historical Data provides charts and reports displaying trends over time.

e. Search Function allows users to locate specific information within DPRO.

f. Subscriptions are automated email delivery of DPRO products and presentations. Subscription delivery schedules are as follows:

(1) Daily subscriptions: between 2000 hrs and 0600 hrs.

(2) Weekly subscriptions: Monday through Friday, between 1800 hrs and 0600 hrs. (Monday's subscription email contains data from the Friday of the previous week.)

(3) Monthly subscriptions: Beginning on the first day of the month, containing end-of-month data for the previous month.

(4) Subscription deliveries will not be scheduled for federal holidays or weekends, but pending deliveries will still be processed.

Chapter 5
Record Brief

5-1. Overview

The Record Brief application is an interface for Army National Guard Human Resource Specialists to review and update Soldiers' Records Brief.

5-2. Access

Access to the Record Brief application is determined by a user's duty position and command hierarchy. To request access:

a. Log into Guard One (formerly known as RCMS-G G-1 Portal) at https://arngg1.ngb.army.mil/.

b. Select the Record Brief application.

c. Select "Request Access" and complete the online form. Select the correct hierarchy and role. Do not select hierarchies outside of Georgia, or a role other than "Record Brief Viewer" or "Record Brief Editor." Incorrect requests may not be processed.

d. Upload a completed DD Form 2875, following the instructions in Appendix C.

5-3. Roles

User roles define the tasks a user can perform within the application.

a. Record Brief Viewer role allows users to view and download Records Brief for Soldiers within their command hierarchy. Most users will be assigned this role.

b. Record Brief Editor role allows users to view, edit and download Records Brief for Soldiers within their command hierarchy. Only HR Professionals (42A, 420A, 42H/B) will be assigned this role.

c. State Admin role allows users to view, edit and download Records Brief for Soldiers within the state. State Admin also approves user access to the application at the state level. This role is exclusive to the User Access Account Administrator.

5-4. Responsibilities

a. G-1 HR Systems Branch manages user access accounts to the application.

b. MSC S-1 ensures subordinate Battalions and units are following this SOP and guidance provided via user manual.

c. Battalion S-1 provides units and Soldiers with Records Brief on annual basis, and updates ADS as necessary in order to update Soldiers' data.

d. Individual Soldiers review and validate their Records Brief via ARNG G1 Personnel Gateway Self Service website (https://arngg1.ngb.army.mil/SelfService/CareerCenter.) Records Brief can only be validated by individuals Soldiers, and this cannot be accomplished via the Record Brief application.

Chapter 6
GA Power App Catalog

6-1. Overview

The GA Power App Catalog is a collection of applications developed on the Microsoft Power App platform and deployed via Microsoft Teams. It aims to streamline processes and improve access to information for all GAARNG personnel at all levels. Direct all questions regarding the GA Power App Catalog to G-1 HR Systems Branch via email at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

6-2. Access

Access to the GA Power App Catalog is automatically determined based on a user's Global Address List (GAL) profile information. Users experiencing access difficulties should update their GAL profile:

a. Visit the ID Card Office Online website (https://idco.dmdc.osd.mil/idco) and select "My Profile."

b. Click the appropriate tab (MIL for military, CIV for Federal Technicians, and CTR for contractors) and ensure the following are correct:

(1) Duty Organization must be "National Guard."

(2) Duty Sub Organization must be "--NG - Army National Guard - Georgia."

c. The system updates GAL information nightly, automatically adding new users to the Teams and granting access to the GA Power App Catalog.

d. Access to individual applications within the GA Power App Catalog is determined by leveraging data from the GA Contacts and GA SAAR Manager applications (paragraph 6-3) to ensure users have a "need-to-know."

6-3. Applications

The GA Power App Catalog includes several interconnected applications designed to enhance efficiency and productivity. This paragraph details only the applications managed by G-1; numerous other applications exist within the catalog that are outside the scope of this SOP.

a. GA Contacts provides a GAARNG-wide directory and manages user roles, which directly impact access and capabilities within other GA Power Apps.

b. GA SAAR Manager Streamlines and automates the DD Form 2875 process for systems managed by the G-1 HR Systems Branch, and directly impact access and capabilities within other GA Power Apps.

c. GA UMR Navigator offers a current view of unit manning and associated personnel information.

d. RCAS Orders Archive provides access to historical personnel orders from the legacy Reserve Component Automation System (RCAS) Military Personnel Office (MILPO) system.

e. GA Separations Manager streamlines separation proceedings within the GAARNG; detailed procedures are outlined in the G-1 HR Services Branch SOP.

f. GA LAB Path tracks cadets from Reserve Officer Training Corps (ROTC) contract through promotion to First Lieutenant, providing a common operating picture for officer tracking.

Chapter 7
SGLI Online Enrollment System (SOES)

7-1. Overview
SOES is the official platform for managing Servicemembers' Group Life Insurance (SGLI) and Family SGLI (FSGLI). It replaces paper-based enrollment, centralizes SGLI/FSGLI data, and provides 24/7 self-service access for eligible active and reserve component Servicemembers. SOES ensures consistent SGLI/FSGLI information for both members and their leadership. Use of SGLV 8286 is obsolete.

7-2. Access
SOES is a national system, and access to the system is not managed by the state.

a. Soldiers access SOES through milConnect using either their CAC or DS Logon at https://www.dmdc.osd.mil/milconnect.

b. To certify or update SGLI elections, navigate to Benefits > Life Insurance (SOES-SGLI Online Enrollment System.)

c. For assistance with DS Logon, utilize the "Help Center" on the upper right corner of the website, or call the DMDC Support Center (DSC) at 800-477-8227.

7-3. Responsibilities
Soldiers are required to make an initial SGLI election upon entry into military service and are strongly encouraged to review and update their elections annually or following significant life events. Responsibilities are outlined below:

a. Battalion S-1

(1) tracks and notifies Soldiers requiring SGLI re-certification;

(2) develops and implements a plan to maintain at least 80% completion rate throughout the fiscal year;

(3) and educates Soldiers on SGLI requirements.

b. Individual Soldiers

(1) complete, update, or re-certify SGLI elections annually or as needed;

(2) and maintain accurate dependent information in Defense Enrollment Eligibility Reporting System (DEERS).

7-4. Timeline
Changes to beneficiary designations, coverage amount increases, and coverage restoration are effective immediately upon certification. However, reductions in coverage and declinations of coverage will not take effect until the first day of the month following certification; the previous coverage amount will remain in effect until then.

Chapter 8
Real-time Automated Personnel Identification System (RAPIDS)

8-1. Overview
RAPIDS is a Department of Defense (DoD) system used to issue the definitive credential within DoD. RAPIDS uses information stored in the DEERS when providing these credentials. Used together, these two systems are commonly referred to as a DEERS/RAPIDS system or DEERS/RAPIDS infrastructure.

8-2. Access
Permissions are determined based on the user's role and the recommendations from the MSC.

a. Users must complete initial or annual re-certification training IAW Appendix E of this SOP. The certification and re-certification training is available via Joint Knowledge Online Learning Management System.

b. Once certification or re-certification training has been completed, users must complete and submit DD Form 2875 and DD Form 2841 on annual basis. Contact G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil for the latest version of templates for each document.

8-3. Roles and Responsibilities
Each MSC S-1 is assigned a deployable RAPIDS site. Each site must maintain two Site Security Managers (SSMs) and as many Verifying Officials (VOs) to accomplish their mission. MSCs coordinate among their Battalions to provide DEERS support within their MSCs.

a. State SSM

(1) serves as liaison between the MSCs, State DEERS/RAPIDS sites, and NGB Service Project Office;

(2) maintains access and processes cases via IPPS-A CRM case;

(3) conducts quarterly review of deployable sites, and addresses any unexplained or unresolved discrepancies with the site's SSM;

(4) reviews and retains copy of site requests for training and verification of new users;

(5) schedules and conducts a minimum of one unannounced DEERS/RAPIDS site visit each calendar year;

(6) monitors site activities to ensure all users are logging in and utilizing the systems at least once a month;

(7) maintains a current personnel roster of system users to include rank, name, system name, and identification of each user's role as a SSM (primary or alternate) or VO;

(8) maintains signed and dated copies of DD Form 2841, Public Key Infrastructure (PKI) Agreement for DEERS/RAPIDS users, on every SSM and VO;

(9) ensures distribution of updates, policy reviews, and information to SSMs of each site;

(10) and performs all roles of the VO and MSC SSM.

b. MSC SSM

(1) maintains signed and dated copies of DD Form 2841 and proof of NACI for each SSM and VO, and provides copies to the State SSM;

(2) notifies the State SSM immediately of any pending SSM or VO personnel change and the site's plan of transition;

(3) ensures the Privacy Act Statement and DD Form 2842 are posted with workstations;

(4) ensures all deployable RAPIDS systems are powered on and connected to VPN regularly to ensure receipt of updates;

(5) ensures all site users log onto the system at least once every thirty days to remain active and complete their annual re-certification requirements;

(6) ensures physical cardstock inventory accurately match the Inventory Logistics Portal (ILP) data and securely stored at the end of each business day;

(7) ensures all expired, terminated, or failed Common Access Cards (CACs) and Uniformed Services Identification (USID) are properly labeled in the front lower right corner of each card;

(8) returns expired, terminated, or failed cardstock to the DMDC Support Center at least monthly, or more often as necessary, to maintain accurate accountability in the ILP;

(9) checks ILP for cardstock discrepancies on monthly basis and notifies the chain of command to initiate a 15-6 investigation when the discrepancy reaches 11 or more (the investigation must be completed within 45 calendar days of report of discrepancy);

(10) ensures used printer ribbons are cross-shredded to safeguard personal information;

(11) and performs all roles of the VO.

c. VO

(1) must be a U.S. citizen and vetted by the personnel security office in accordance with DoD 5200.2-R to meet the requirements for holding IT-II position as described in DoD Directive 8500.1 (favorable NACI);

(2) verifies of identity of all Servicemembers (SMs) and beneficiaries through available supporting documentation when updating records and issuing CACs or USIDs;

(3) and properly labels all returned CACs and USIDs in the front lower right corner.

Chapter 9
Interstate Transfer (IST)

9-1. Overview
IST is a process of transferring a Soldier from one state to another state within the Army National Guard. This process ensures continuity of service, benefits, and pay for Soldiers transferring into or out of the GAARNG. Coordination and approval are managed by State IST Coordinators, with administrative routing occurring outside of IPPS-A via official email, Microsoft Teams, or the Retention Management System (RMS), based on established state procedures.

9-2. Inbound Transfers
Inbound ISTs occur when a Soldier from another state transfers into the GAARNG. The gaining state (GAARNG) is responsible for initiating coordination and confirming eligibility.

9-3. Outbound Transfers
Outbound ISTs occur when a GAARNG Soldier transfers to another state's Army national Guard. The losing state (GAARNG) is responsible for validating eligibility, and releasing the Soldier after coordination and acceptance from the gaining state.

9-4. Responsibilities
a. State IST Coordinator for Outbound Transfers

(1) validates Soldier's eligibility and confirms that all documents listed in paragraph 10-4 are current and complete;

(2) ensures no open personnel actions, pay issues, or flags remain in IPPS-A;

(3) provides written coordination and confirmation to the gaining state prior to releasing the Soldier;

(4) and closes the Soldier's assignment in IPPS-A only after confirmation of acceptance from the gaining state.

b. Losing Unit and Battalion S-1

(1) compiles and verifies the complete IST packet;

(2) ensures Soldier is briefed on transfer timelines and responsibilities;

(3) and uploads all required documentation into iPERMS as appropriate and confirms synchronization in IPPS-A.

c. Transferring Soldier

(1) coordinates directly with the gaining state IST Coordinator to provide all necessary documents;

(2) confirms receipt of transfer orders and reporting instructions;

(3) and continues communication with the unit and Battalion S-1 until the new assignment in gaining state is finalized.

d. If Soldier is in Active Guard Reserve (AGR) program, IST transfers must be coordinated through the HRO and respective program managers to ensure proper authorization and release from Title 32 AGR program.

e. If Soldier is an Officer or Warrant Officer, IST transfers are managed by the Recruiting and Retention Battalion (RRB) Officer Strength Management (OSM) section. Officers and Warrant Officers will follow the guidance published in the GAARNG Officer Strength Management SOP for packet preparation, coordination, and submission.

9-5. Required Documents
All IST packets, both inbound and outbound, must include the following documents. These documents ensure eligibility verification, administrative continuity, and accurate processing of the assignment within IPPS-A.

a. DA Form 4187, Request for Personnel Action (annotated for Interstate Transfer)
b. Current SRB, generated from IPPS-A
c. Most recent NCOER/OER (last two rating periods, if applicable)
d. DA Form 705, AFT (or ACFT) Scorecard, or current AFT record from DTMS
e. DA Form 5500/5501, Body Fat Content Worksheet, if applicable
f. Most recent physical exam (must be within 12 months)
g. Copy of Active Duty orders, if applicable (ADOS or AGR status)
h. Copy of Valid Driver's License or CAC (for identity verification)
i. Security Clearance Verification (DISS printout or Memorandum from the Personnel Security Office)
j. DA Form 5016, Retirement Points Statement, generated from IPPS-A
k. Letter of Acceptance (or Endorsement) from the gaining unit commander
l. Verification of Civilian Employment, if applicable (for M-Day Soldiers)
m. Any other documents deemed necessary at the discretion of the IST Coordinators

9-6. Procedure

a. Inbound to GAARNG

(1) Soldier contacts the GAARNG State IST Coordinator expressing intent to transfer into the organization.

(2) G-1 HR Systems Branch provides the Soldier with the GAARNG IST Packet Checklist and validates available positions within the state.

(3) Soldier submits the completed IST packet with all documents listed in paragraph 10-4.

(4) G-1 HR Systems Branch reviews submitted IST packet for accuracy and completeness; coordinates with the gaining unit commander for Letter of Acceptance (or endorsement) and confirms MOS eligibility.

(5) Upon approval, the losing state creates the assignment in IPPS-A, using the effective date agreed upon by both states.

(6) State IST Coordinator arrives Soldier to the new assignment and notifies the Soldier and the losing state of acceptance.

(7) Soldier reports to the assigned unit as directed.

b. Outbound from GAARNG

(1) Soldier notifies the GAARNG State IST Coordinator of intent to transfer to another state.

(2) G-1 HR Systems Branch provides the Soldier with the IST Packet Checklist and validates that all required documents are current.

(3) The losing unit and Battalion S-1 ensure the Soldier's personnel and pay records are current in IPPS-A and iPERMS.

(4) G-1 HR Systems Branch forwards the IST packet and confirmation of eligibility to the gaining state.

(5) Upon receipt of written confirmation from the gaining state, the G-1 HR Systems Branch creates a new assignment in the gaining state in IPPS-A and provide a confirmation of release to the Soldier and the losing unit.

(6) All technical issues or data synchronization errors will be reported through CRM to the provider group "NGGA G-1 HR Systems Branch" for resolution.

c. Post-Transfer Actions

(1) The gaining unit initiates local in-processing actions to include but not limited to ID card update, finance, security, and medical review.

(2) The losing unit ensures no pending administrative or pay discrepancies remain in IPPS-A.

(3) Both gaining and losing states confirm completion of assignment and strength accountability through DPRO or other authorized reporting tools.

Appendix A
References

Section I
Publications

AR 140-185
Training and Retirement Points

AR 25-22
The Army Privacy Program

AR 380-5
Army Information Security Program

AR 600-8-14
Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel

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

DA PAM 600-8-104
Army Military Human Resource Records Management

DoD 1000.30
Reduction of Social Security Number (SSN) Use within DoD

DoD 1341.14
Servicemembers' Group Life Insurance (SGLI) On-line Enrollment System (SOES)

DoD 5200.2-R
Personnel Security Program

NGR 680-2
Automated Personnel Data System

PPOM #13-028
Authority for Removal of iPERMS Documents

PPOM #15-019
State Interactive Personnel Electronic Records Management System (iPERMS) Domain Management Guidance

PPOM #18-040
System Authorization Access Request with Favorable Background Investigation Required to Access Personnel Systems within the ARNG HR Domain

Section II
Forms

DD Form 2875
System Authorization Access Request (SAAR)

DD Form 2841
Department of Defense (DOD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities

DA Form 93
Record of Emergency Data

Section III
Abbreviations

AGR
Active Guard/Reserve

AMHRR
Army Military Human Resource Record

AOC
Area of Concentration

ARNG/ARNGUS
Army National Guard / Army National Guard of the United States

ASI
Additional Skill Identifier

ASVAB
Armed Services Vocational Aptitude Battery

CAC
Common Access Card

CRM
Customer Relationship Management

DEERS
Defense Enrollment Eligibility Reporting System

DA
Domain Administrator

DM
Domain Manager

DMDC
Defense Manpower Data Center

DoD
Department of Defense

DPRO
Directors Personnel Readiness Overview

DL
Distance Learning

DSC
DMDC Support Center

EAD
Enter into Active Duty

ERP
Early Retirement Pay

FSGLI
Family Servicemember's Group Life Insurance

HR
Human Resource

HRO
Human Resource Office

HRC
Human Resource Center

HSS
Health Services Section

IDES
Integrated Disability Evaluation System

IFT
Instructor Facilitated Training

IPPS-A
Integrated Personnel and Pay System - Army

iPERMS
Interactive Personnel Electronic Records Management System

MILPO
Military Personnel Office

MSC
Major Subordinate Command

MOS
Military Occupational Specialty

NACI
National Agency Check with Inquiries

NGB
National Guard Bureau

PAR
Personnel Action Request

PEO EIS
Program Executive Office, Enterprise Information Systems

PKI
Public Key Infrastructure

RAD
Return from Active Duty

RAPIDS
Real-time Automated Personnel Identification System

RCAS
Reserve Component Automation Systems

RPAM
Retirement Points Accounting Management

RPED
Retirement Pay Eligibility Date

SAAR
System Authorization Access Request

SGLI
Servicemembers' Group Life Insurance

SQI
Special Qualification Identifier

SSM
Site Security Manager

SOES
SGLI Online Enrollment System

UMR
Unit Manning Report

VO
Verifying Official

VPN
Virtual Proxy Network