GAARNG Standard Operating Procedures

Human Resource Systems Branch (NGGA-PES)

Human Resource Systems

Joint Force Headquarters
Georgia Army National Guard
Marietta, GA
15 October 2024

Contents

Chapter 1 Introduction

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

Chapter 3 Interactive Personnel Electronic Records Management System (iPERMS)

Chapter 4 GuardSuite

Chapter 5 Directors Personnel Readiness Overview (DPRO)

Chapter 6 Record Brief

Chapter 7 Reserve Component Automation Systems (RCAS)

Chapter 1
Introduction

1-1. Purpose: This Standard Operating Procedures (SOP) provides policies and procedures for Georgia Army National Guard's (GAARNG) Soldiers utilizing Human Resource (HR) Systems. This document covers access management, managing, and updating personnel records via various HR Systems. Each state operates independently to uphold polices, rules and procedures set forth by National Guard Bureau (NGB) and Human Resource Center (HRC) as it relates to management program to accurately represent a Soldier's military service.

1-2. Scope: All personnel employed to support the administrative functions in the GAARNG will adhere to policies and procedures set forth herein. This document will encompass complete administrative operations and other recurring tasks that will be standardized and made routine. Additionally, all personnel will conform to accept procedures and standards as published or implied in the Army National Guard and Department of Army directives applicable to the Army National Guard.

1-3. Privacy Act: Army Military Human Resource Record (AMHRR) custodians and authorized officials will use the Army Privacy Program to safeguard the right to privacy of present and former military members. No person is entitled to obtain information from or possess AMHRRs solely by virtue of his or her position. The AMHRR contains privileged material and will be made available to authorized personnel when required in the performance of official business.

Prior to releasing any Soldier's information or documents pertaining to a Soldier to any person outside the GAARNG, the user will obtain a consent to release of information signed by the Soldier. The user will verify the signature against another signed document for authentication.

All AMHRRs are CONTROLLED UNCLASSIFIED INFORMATION unless they are classified higher IAW AR 380-5. Classified AMHRRs must and will be protected to prevent unauthorized access or disclosure.

1-4. Fraud and Forgery: Fraud and forgery is something that occurs at all levels and is done by Soldiers of all ranks. It degrades the integrity of Army systems, and it negates multiple Army Values. It should be taken seriously by all system users and leaders, as well as individual Soldiers. Report fraud and forgery immediately to G-1 HR Systems Branch via ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

If fraud or forgery is confirmed, the user's accounts will be suspended, and Soldier(s) will be reprimanded as the commander sees fit. G-1 HR System Branch will correct HR systems with the appropriate data.

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

2-1. Overview: IPPS-A is a Web-based HR system that provides integrated personnel and pay capabilities and a comprehensive HR record for all Soldiers in each Component of the Army. GAARNG went live November 2019 with some functionally. IPPS-A underwent another transformation in January 2023 with Regular Army and Army Reserve joining the system. More functionally will come with future transformations, and once IPPS-A is fully deployed, the system will enable HR transactions to automatically trigger Soldier pay. In addition, Soldiers now have access to their own personal information 24 hours a day via the IPPS-A Self-Service Web Portal.

IPPS-A's ability to combine personnel and pay functions (e.g., a promotion or call to Active Duty) will address current inefficiencies caused by complex interfaces among more than 40 "stove-piped" HR systems. As a result, IPPS-A will leave fewer opportunities for error and will become the authoritative and comprehensive source of Army personnel and pay information.

2-2. Access: GAARNG Soldiers automatically have basic user access for Self Service within IPPS-A. Users who are having difficulty accessing IPPS-A will contact G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil for resolution. Elevated user access for all personnel employed to support the administrative functions in the Georgia Army National Guard will be requested and managed in accordance with this SOP.

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

b. Users requiring elevated access 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 (link above) to complete DL, then schedule themselves for an IFT course within Microsoft Teams (GAARNG G1 Systems Support.)

(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 have 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.

d. Elevated user access accounts will be automatically or manually de-provisioned in the event one of the following occurs. If users need access restored, 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: Elevated user access within IPPS-A is composed of two different parts: Roles and Permissions. Appendix B shows appropriate Category, Subcategory, and Row Security settings.

a. Roles are which specific tasks and/or actions users can perform within the system. Users' roles are determined by the three available basic categories, and specific subcategories within.

(1) Member: Self-service access to Personnel Action Requests, open and manage Helpdesk cases, enroll in and manage completion of IPPS-A training, set enlisted promotion preferences; view access to contract data, duty status, orders, Soldier Record Brief, security clearance information, physical exams, PULHES, award record, Integrated Disability Evaluation System (IDES) information, promotion point worksheet, promotion point allocation, dependent/beneficiary information, training information, talent profile (Awards, Licenses & Certifications, Career Management, Education, Qualifications, Language, Skills).

(2) HR Professional: Access to submit PAR requests on behalf of a Member, delegation of PAR request, manage decentralized enlisted promotion rosters, perform benefits administration functions and benefits enrollment, manage assignments, update departure and/or arrival information, update awards, licenses & certifications, aviation, career management, education, qualifications, language, and skills, view Human Resource Authorization Report and update a Member's position, view military training information, view and maintain additional security clearance attributes, update duty status of Members for those transactions that do not have a HR event trigger, administer personnel restrictions and flags, view physical profiles, deployment readiness, line of duty, Helpdesk dashboard, 360-Degree View, create a case, predefined queries, view the department security tree, view orders, perform approval of workflow transactions within the S1 Pool, ad hoc additions and removing of users within the S1 pool, reassign workflow transactions, monitor workflow approval process, administer workflow and setup templates.

(3) Commander: Access to personnel actions, special pay and leave requests; view Members' dependent and beneficiary information, benefits enrollment, security clearance, duty status, emergency contact information, personnel restrictions, Soldier Record Brief, nine predefined queries, Integrated Disability Evaluation System (IDES) information, roster of members with P3 or P4 in their PULHES, talent profile, training summary, talent summary, orders, position information, physical exams, physical qualifications, deployment readiness, line of duty, involuntary and voluntary separation, military training, non-person profiles Aviation, Job Code (MOS/MOSW/AOC), strength management information, military education level, Physical Profiles (PULHES, ACFT), Qualifications (PRP, ASVAB), Skills (SQI, ASI), etc. Additionally,

manually update the flag tab of the restrictions page (initiate, transfer, remove), maintain and manage direct report users associated with decentralized boards, review the Promotion Eligibility Roster and promote the Member, approve workflow requests, recommend approval or denial of personnel action requests and provide comments; recommend approval/denial, or approve/deny recommendation for awards, review and comment on workflow requests, view and approve direct reports IPPS-A training.

b. Permissions are specific group(s) of Soldiers for whom users may see and perform actions within IPPS-A. Permissions are determined by a UIC or a rollup UIC. Users will only be given permissions to Soldiers within their command hierarchy.

2-4. IPPS-A Audits: The integrity of Soldier data that drives all personnel and pay actions is paramount and all transactions within the system are logged. Specific behaviors are monitored within the state in order to help prevent and identify individuals who are attempting to commit fraud or abusing the rights afforded to those with access to IPPS-A. Consequences for violating written policies (Appendix B, section I) will be managed by G-1 HR Systems Branch. G-1 HR Systems Branch will maintain the violations for one year and execute the following actions:

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

b. User’s second violation will result in suspension of access until the Brigade S1 communicates with the G1. The G1 and Brigade S1, will determine when the user will receive access back. This decision will be based on the severity of the user’s action.

c. User’s third violation will result in suspension of access, along with user retraining provided quarterly. Furthermore, the G1, Brigade Administrative Officers, and Chief of Staff will communicate the issue and discuss any future action for the user.

2-5. Workflow Templates: Allows HR Professionals the ability to maintain the flow of their personnel action request. Once a workflow template is built and created, it can be shared for use by other users. MSC/BN S-1 are expected to review these workflows monthly in order to maintain updated and relevant workflows. Request for assistance with updates or creation can be submitted via Microsoft Teams in GAARNG G1 Systems Support channel (see Appendix B) or email to ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

2-6. S1 Pool: The S1 Pool is a group of HR Professionals used as the default workflow routing for all actions. Instead of routing to a specific user, requests are routed to a pool of users. The “S1 Pool” are set up and maintained manually. Submit request to HR Systems Branch via Microsoft Teams in GAARNG G1 Systems Support channel (see Appendix B) or email to 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 listed below.

a. State HR Systems Branch:

(1) Manages user access accounts within IPPS-A.

(2) Provides IPPS-A support (Appendix B).

(3) Manages all Enter into and Return from Active Duty (E/RAD) transitions.

(4) Conducts weekly audits IAW Internal Control Compliance Guide.

b. <u>State Human Resource Office (HRO):</u>

(1) Manages actions required for Title 32 Active Guard Reserve (AGR) Soldiers.

(2) Manages actions required for Title 32 Technicians

c. <u>Brigade S-1 Office:</u>

(1) Processes personnel actions IAW this SOP.

(2) Conducts monthly review of user access accounts, PAR workflows, and S1 pools within their Brigade.

(3) Maintains personnel action processes for Brigade and below transactions

d. <u>Battalion S-1 Office:</u>

(1) Processes personnel actions IAW this SOP.

(2) Monitors and processes all personnel actions within S-1 Pool.

e. <u>Soldiers:</u>

(1) Reviews and updates personnel data.

(2) Notifies unit's chain of command of data discrepancies.

2-8. References:

a. IPPS-A User Manual, Provided by G-1 HR Systems Branch

b. Appendix A – References

c. Appendix B – Authority within Integrated Personnel and Pay System – Army (IPPS-A)

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 having difficulty 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 additional 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 access 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. For questions regarding required role(s) for a specific duty position, contact designated Domain Administrator.

(2) Annually completed DD Form 2875 IAW Appendix C.

(3) New DD Form 2875 completed IAW Appendix C is required if a user is moved from one unit to another within IPPS-A. iPERMS will auto terminate their elevated role(s) and rule(s).

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 Domain Administrators (DAs).

d. Users at all other state staff directorate or users who require Domain Administrator 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. Domain Administrators will only assign user role or rule IAW Appendix D. For any and all exception that is not specifically addressed in Appendix D (e.g., Scan Operator or 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 will be granted based on the user's positions and requirements to complete their assigned mission. See Appendix D for details.

a. Authorized Official (AO): Authorized Officials only have access to view selected records and document types. They will not have access to General Officer Records, Health and Dental Folders, or the Restricted Folder.

b. Field Operator (FO): The Field Operator role provides the capability for a user to input document images into the iPERMS system without requiring specific index information for the correct domain, document name, or effective date. Documents can be uploaded by web scanning the images or web uploading the images from a file.

c. Scan Operator (SO): Scan Operator 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. Data entry is optional and will be re-validated in the next step of the workflow.

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

e. Verifier (VR): The Verification process is used to verify that the data entered during Index/Validation is accurate. The Verification Operator will compare the data entered by the Index Operator with the data on the document image.

f. Quality Control (QC): The QC Operator has the ability to view and process batches grouped in their individual workflow queues, including Index/Validation, Verification, Quality Control, Rescans, Release in Progress and Input Pending. Only HRS, JFHQ and MSC level users will be granted the QC Role.

g. Problem Resolver (PR): Problem Resolver has the ability to resolve and create problem cases in iPERMS. Problems cases are created by Authorized Official, Record Manager, Problem Resolver and State iPERMS Domain Manager/Administrator roles.

h. Domain Administrator (DA): Domain Administrators act as the records manager and mange users within their command hierarchy. Only two users per Brigade will be granted DA Role, typically the Brigade's HR Technician and their designee.

i. Records Manager (RM): Record Managers have access to view selected records and document types as well as review and complete personnel record reviews.

j. Domain Manager (DM): State iPERMS Domain Managers manage problem cases and ensure users are resolving cases. DMs can pull audit reports and manage DAs within the State.

k. Soldier: Individual Soldiers may view and download their own documents and report problems with their files. Soldiers can access their records through AKO.

3-4. Responsibilities: All users will have access to their own iPERMS records. The following sections or individuals are responsible for the information listed below.

a. State G-1:

(1) Manages DM/DA Access.

(2) Processes all batches that are named "RMS Duplicate Document Case Resolution" by re-indexing correctly. These batches are from PR cases sent to QC for corrections.

b. Brigade S-1:

(1) Manages user access IAW Appendix D.

(2) Verifies and processes all batches from subordinate battalions and units.

(3) Processes all batches in the Brigade QC role.

(4) Ensures subordinate battalions and units are completing all required iPERMS actions.

c. Battalion S-1:

(1) Processes all batches in the battalion Personnel Services Specialist's designated roles on a consistent basis.

(2) Verifies all batches from subordinate units.

(3) Ensures records management is taking place in all subordinate units.

(4) Receives and reviews iPERMS user requests, ensuring completeness prior to forwarding to Brigade.

(5) Forwards all approved requests for access to the Brigade Personnel Services Specialists.

d. Unit Personnel:

(1) Scans and Indexes all documents created at the unit level into iPERMS.

(2) Gives Soldiers the opportunity to an annual personnel records review, and ensure all updated documents are then scanned and indexed into iPERMS. See paragraph 3-5 and Appendix E for more information.

(3) Identifies all documents in the Soldier's AMHRR that do not belong to that Soldier, and use the "Report a Problem" tool for document corrections.

3-5. Personnel Record Review: Proper management of Soldiers' AMHRR is crucial in managing Soldiers' career advancement and entitled pay and benefits. Units will ensure all assigned Soldiers' documents in their AMHRR are properly filed and current. This is accomplished via iPERMS Personnel Record Review process. The iPERMS Personnel Record Review is to be performed for all Soldiers on annual basis, and upon arrival to the unit. See Appendix E for instruction on how to perform Personnel Record Review.

3-6. References:

a. AR 25-22, THE ARMY PRIVACY PROGRAM

b. AR 600-8-104, ARMY MILITARY HUMAN RESOURCE RECORDS MANAGEMENT

c. DA PAM 600-8-104, ARMY MILITARY HUMAN RESOURCE RECORDS MANAGEMENT

d. DoD 1000.30, REDUCTION OF SOCIAL SECURITY NUMBER USE WITHIN DOD

e. PPOM #13-028, AUTHORITY FOR REMOVAL OF IPERMS DOCUMENT

f. PPOM #15-019, STATE INTERACTIVE PERSONNEL ELECTRONIC RECORDS MANAGEMENT SYSTEM DOMAIN MANAGEMENT GUIDANCE

g. Appendix A – References

h. Appendix C – Preparation and Submission of DD Form 2875

i. Appendix D – Managing User Access and Batch workflow within iPERMS

j. Appendix E – Completing Personnel Records Review within iPERMS

Chapter 4
GuardSuite

4-1. Overview: GuardSuite is a tool provided to GAARNG users for quick access to personnel data with understanding any inaccurate data need to be managed within IPPS-A.

4-2. Access: Permissions are determined based on the user's role and command hierarchy. Users will not be granted access above their assigned hierarchy. Only exceptions to this rule are Administrative Officers, Executive Officers, S1, HR Technicians, and NCOICs, as they are authorized high headquarters access within GuardSuite.

a. GuardSuite can be accessed using Microsoft Edge at https://nggac2v-dpiiis.ng.ds.army.mil/GuardSuite

b. Submit DD Form 2875 IAW Appendix C annually to G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@army.mil through MSC HR Technicians (for users at MSC level or below) or Section OIC/NCOIC (for users at state staff directorate.)

4-3. Roles: Users will be granted basic viewing rules within GuardSuite.

4-4. References:

a. Appendix A - References

b. Appendix C - Preparation and Submission of DD Form 2875

Chapter 5
Directors Personnel Readiness Overview (DPRO)

5-1. Overview: DPRO is a comprehensive management information system. It provides access to thousands of metrics that are updated daily and available for both current and historical dates. These metrics enable custom reporting in the areas of strength management, attrition, retention, accession, and military readiness. DPRO receives information from dozens of primary data sources.

5-2. Access: Permissions are determined based on the user's role and command hierarchy level. Request for user access account for DPRO requires submission of a completed DD Form 2875 within the website by following the following steps:

a. Log into DPRO at https://arngg1.ngb.army.mil/Portal/.

b. Select DPRO as the application.

c. Select request access and complete the online form. Be sure to select the correct hierarchy and role within the online request. No user shall select hierarchy above or outside state of Georgia, or State User or State Power User role. The request submitted without regards to guideline provided in this SOP may not be accessible by the state's User Access Account Administrator.

d. Attach DD Form 2875, completed IAW Appendix C.

5-3. Functions/Features: The following describes the common functions and features accessible within DPRO. More detailed lists are found within the site's user guide:

a. Dashboards: A visual collection of measurements that is automatically updated on a regular basis, and is either predefined or customized by the user.

b. Leadership Reports: Pre-configured reports available for access to all DPRO users. These reports provide quick and easy access to the reports that the average DPRO user will most frequently use.

c. Views: Show metrics and trend data from a collection of metrics organized around a theme.

d. Historical Data: Preconfigured charts and reports that track the value of selected metrics over time. They provide users with the ability to quickly see how the values of key metrics have changed over a time-frame of choice.

e. Search Function: With the embedded search engine, found on the far-right end of the DPRO Ribbon Toolbar, users can perform search for desired information throughout DPRO with a term or phrase.

f. Subscriptions: DPRO provides access to many products and presentations through a subscription service that automatically sends the selected item(s) to user's enterprise email account.

(1) Daily subscriptions are sent daily between 2000 hrs and 0600 hrs.

(2) Weekly subscriptions are sent Monday through Friday, between 1800 hrs 0600 hrs. (Monday's subscription email contains data from the Friday of the previous week.) If there are still weekly subscriptions in the queue after 6 a.m., they will be sent the following day(s) until all jobs have processed.

(3) Monthly subscriptions are sent beginning on the first day of each month and continue until all subscriptions are sent (meaning some users may receive their subscription on the second or third day of the month or later.) Monthly subscriptions contain end of month data for the previous month. If a user creates this type of subscription in the middle of the month, they will receive one subscription immediately containing the data for the previous month. The job will then be scheduled as a normal Monthly subscription.

(4) No new subscriptions will be generated on holidays and/or weekends, but any subscriptions that are still pending from the previous day will be sent.

5-4. References:

a. Web-friendly user guide within DPRO (found in the Help menu located in the Ribbon Toolbar.)

b. Appendix A - References

c. Appendix C - Preparation and Submission of DD Form 2875

Chapter 6
Record Brief

6-1. Overview: The Record Brief application is an administrator's interface for Human Resource Specialists within the Army National Guard to review and update the Records Brief of Soldiers assigned to their Units.

6-2. Access: Permissions are determined based on the user's role and command hierarchy level. Request for user access account for Record Brief requires submission of a completed DD Form 2875 within the website by following the following steps:

a. Log into record brief at https://arngg1.ngb.army.mil/Portal/.

b. Select Record Brief as the application.

c. Select request access and complete the online form. Be sure to select the correct hierarchy and role within the online request. No user shall select hierarchy above or outside state of Georgia, or Record Brief Viewer or Record Brief Editor role. The request submitted without regards to guideline provided in this SOP may not be accessible by the state's User Access Account Administrator.

d. Attach DD Form 2875, completed IAW Appendix C.

6-3. Roles: User role determines what you can do in Record Brief. There are several Record Brief roles:

a. Record Brief Viewer: Allows users to view Records Brief for Soldiers in their assigned command hierarchy. This is the role most Record Brief users are assigned.

b. Record Brief Editor: Allows users to view and edit Record Brief contents for Soldiers in their assigned command hierarchy.

c. Super Editor: Allows users to view and edit Record Brief contents for Soldiers in their assigned command hierarchy. They may also be given the permissions to manage other user's access accounts to Record Brief.

d. Admin: Allows users to view and edit Record Brief contents, and manage other user's access accounts to Record Brief for Soldiers and users within their assigned command hierarchy.

6-4. Versions: There are four versions of a Soldier's Record Brief that can be viewed within the product:

a. Record Brief: Contains the most up-to-date data available within the product, and is viewed by clicking either the Download Record Brief or Download Selection Board option.

b. Validated Record Brief: Reviewed and verified by the Soldier that everything is accurate. Users need to be aware that Validated Record Brief may contain different data from Record Brief. This is because a snapshot of the Record Brief data is taken and saved within the system at the time it is validated. This means that although the record is constantly being updated, the validated Record Brief information remains unchanged until it is validated again.

c. Certified Record Brief: Certified by a Human Resource Specialist that the Soldier's Record Brief has been reviewed and verified for accuracy, and is current. While the ideal progression is for the Record Brief to be certified after it has been validated by the Soldier, a Human Resource Specialist may certify a Record Brief that has not previously been validated by the Soldier, to make it available for a Board.

d. Selection Board Record Brief: Mimics what a Board sees on a Soldier's Record Brief. This redacts certain personal information that is irrelevant for a board.

6-5. Responsibilities:

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

b. Brigade S-1 ensures subordinate commands 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 authoritative data source as necessary IOT update Soldier’s data.

d. Soldier: reviews and validates via ARNG G1 Personnel Gateway Self Service website (https://arngg1.ngb.army.mil/SelfService/CareerCenter). Records Brief can only be validated by individual Soldiers, and this cannot be accomplished via the Record Brief Application.

6-6. References:

a. Record Brief User Guide, found within Record Brief.

b. Appendix A - References

c. Appendix C - Preparation and Submission of DD Form 2875

Chapter 7
Reserve Component Automation Systems (RCAS)

7-1. Overview: RCAS is a combination of applications and equipment that helps you perform some of your tasks as a member of the Army National Guard (ARNG). RCAS is a Department of the Army (DA) organizational element within the Program Executive Office, Enterprise Information Systems (PEO EIS), and Integrated Personnel and Pay System - Army (IPPS-A) program office is the Army proponent for RCAS. RCAS provides a modernized system for performing your day-to-day jobs as well as new functionality.

7-2. Access: Permissions are determined based on the user's role and command hierarchy level.

a. Initial access require users must login https://nggac2-app01.ng.ds.army.mil/RCASWeb and "Request Access" in the upper right hand corner of the website.

b. Users will complete and submit DD Form 2875 annually IAW Appendix C.

7-3. Applications: There are two main applications utilized within RCAS.

a. Retirement Points Accounting Management - Next Generation (RPAMNext): An application that creates and updates records of retirement points for members of the Army National Guard. The application is managed by G-1 HR Systems Branch, and allows users to maintain the retirement point accounts of individual Soldiers; qualify Soldiers for non-regular retirement; import and validate data from external system such as IPPS-A; import to and export from other states for Soldiers who move from one state to another; generate more than 20 various reports, forms, and letters including NGB Forms 23A, 23A1, 23B, 23C, 23D, 23E, and 23F; and determine eligibility for Reduced-age Retirement Pay, and calculate and display the Retirement Pay Eligibility Date (RPED) for Soldiers. See Appendix F for more details regarding RPAMNext.

b. NGB22: An application that creates and publishes the NGB Form 22 (National Guard Report of Separation and Record of Service) upon Soldier's separation from the National Guard. The application provides a wizard that helps streamline the process of generating the NGB Form 22.

7-4. References:

a. RCAS Web Administration Software User Manual (SUM), found within RCAS at https://nggac2-app01.ng.ds.army.mil/sum/RCASWEBSUM.pdf.

b. Appendix A – References

c. Appendix C – Preparation and Submission of DD Form 2875

d. Appendix F – Management of Retirement Points Records within RPAMNext

Chapter 8
GA Power App Catalog

8-1. Overview: GA Power App Catalog is a bundle of many different application developed in the Microsoft Power App platform and deployed via Microsoft Teams. It is aimed to allow for more organized management of processes as well as easier access to and analysis of information for employees of the GAARNG in all capacities at all echelon levels. All questions regarding GA Power App Catalog should be addressed to G-1 HR Systems Branch via email at ng.ga.gaarng.list.g1-human-resource-systems@army.mil.

8-2. Access: GA Power App Catalog is designed to automatically determine the user's accessibility based on the user's profile information in Global Address List (GAL.) Users who cannot access GA Power App Catalog in their Microsoft Teams need to have their profile information updated. In order to update GAL profile, visit ID Card Office Online website at https://idco.dmdc.osd.mil/idco/ and choose "My Profile" option. Then click appropriate tab (MIL, CIV, or CTR) to update the following:

a. Duty Organization must be "National Guard."

b. Duty Sub Organization must be "--NG - Army National Guard - Georgia."

The system receives updated GAL profile information each night to determine users' accessibility, and automatically add new users to the Teams, making the GA Power App Catalog available to users for access.

8-3. Applications: GA Power App Catalog has many different applications deployed to help users improve efficiency and productivity, and those applications are designed to rely on one another for their functionality.

a. <u>GA Contacts</u>: This application serves as the address book for the Georgia Army National Guard employees. It allows users to view a list of members (both Soldiers and civilian employees) of an organization and their contact information. Users have ability to narrow down the search results to specific MSC, BN, and unit, or they may search by a specific role and/or name of the member. Choosing a specific member from the search result will display the following information:

(1) Profile information from GAL.

(2) Roles in the Organization: Users may add a role (or multiple roles as appropriate) to a specific member as appropriate. Roles with three verifications from different users will become verified roles for the member. This function allows for easy identification of employees in specific capacities and positions, and some of the members' roles identified in this application have impacts on the members' accessibility to some of the other applications as explained in this chapter. It is highly encouraged that brigade and battalion administrative officers take time to accurately identify their employees with their assigned roles/position within the organization.

(3) Documents: DA Forms 2875 (SAAR) completed using the GA SAAR Manager application will be available for view. Users may also upload other documents such as completion certificates of Cyber Awareness Training and DoD CUI Certificates.

b. <u>GA SAAR Manager</u> allows for streamlined completion and submission of the DA Forms 2875 by automating routing of SAARs through involved parties from a requestor all the way to the system administrator. It provides users with email notification when user action is required, visibility on submitted SAARs' progress within the application, and allows for easy management of completed SAARs. The SAARs for all systems managed by the G-1 HR Systems Branch are only to be submitted and accepted via GA SAAR Manager application. Users may have up to four different pages within the application, depending on user's position and assigned role(s) in GA Contacts application. See Appendix C for more details.

(1) My SAAR page is available to all users. A user will use this page to initiate a new SAAR, identify a supervisor by email address, and submit it for further processing. Once submitted, user will be able to view the progress of submitted SAARs. This page also provides users with access to all completed SAARs.

(2) Supervisor page is available to all users. A user identified as a supervisor on a submitted SAAR will have access to it for action. A supervisor will review the SAAR, identify the security manager by email address, and deny or approve the request. If denied, the workflow of the SAAR will be terminated. If approved, it will generate and send an email notification to identified security manager.

(3) Security Manager page is available to users who are identified with Security Manager role within the GA Contacts application. A security manager will review and validate requestor's security clearance status.

(4) System Admin page is for users who are identified with one or more System Admin role(s) in the GA Contacts application. Users with this role will grant final approval or denial for a submitted SAAR. A system admin will approve or deny the request. If approved, he or she will take appropriate action to provision user access accounts.

c. GA Contacts Tracker is a Microsoft Power BI analytic tool designed to provide users with overall status of roles added to employees within the GA Contacts application. Brigade and battalion administrative officers are encouraged to review this information on regular basis to determine whether updates to information in GA Contacts application are necessary.

d. GA UMR Navigator provides information on an organization's manning in a manner similar to that of legacy Unit Manning Reports (UMR). Users may select a specific unit to view a list of all positions available in the selected unit, as well as assignments associated with each position. Selecting a Soldier within this application provides access to the individual's personnel information. In order to access this application and its information, a user must have a "GA Power Platform – Personnel Data Viewer" SAAR submitted and approved via GA SAAR Manager application. See Appendix C for more information.

e. GA RCAS Orders Archive: This application serves as the archive repository of all historical orders published within the legacy RCAS Military Personnel Office (MILPO) system. In order to access this application and its information, a user must have a "GA Power Platform – Personnel Data Viewer" SAAR submitted and approved via GA SAAR Manager application. See Appendix C for more information.

8-4. References:

a. Appendix A – References

b. Appendix C – Preparation and Submission of DD Form 2875

Chapter 9
SGLI Online Enrollment System (SOES)

9-1. Overview: SOES is the Servicemembers' Group Life Insurance (SGLI) On-Line Enrollment System. It replaces the paper-based SGLI/Family SGLI (FSGLI) enrollment, maintains elections and beneficiary information, and provides 24/7 self-service access to SGLI information. SGLI provides insurance coverage to eligible members of the active and reserve components. SOES centralizes SGLI/FSGLI data into one authoritative system capable of providing consistent SGLI/FSGLI information to members and their leadership. Use of SGLV Form 8286 is no longer permitted.

9-2. Access: SOES access is not managed by the state.

a. All service members can log into milConnect with their CAC or with their DS Logon at www.dmdc.osd.mil/milconnect.

b. To see and update SGLI elections, after user logs into milConnect, navigate to Benefits, Life Insurance (SOES-SGLI Online Enrollment System.)

c. For online assistance with DS Logon, click “Help Center” on the upper right corner of the website. For assistance by telephone, call the DMDC Support Center (DSC) at 800-477-8227.

9-3. Responsibilities: SGLI is to be updated upon initial entry into military service, and as changes occur. It is highly encouraged that the SGLI certification is reviewed at least on annual basis. The following sections or individuals are responsible for the information listed below.

a. Battalion S-1 Office:

(1) Tracks and notifies Soldiers requiring updated SGLI.

(2) Develops a plan to maintain 80% updated throughout the fiscal year.

(3) Educates Soldiers on the requirements for a SGLI.

b. Soldiers:

(1) Complete initial SGLI or update as needed. Actions include but not limited to:

(a) Increase, reduce or cancel SGLI and FSGLI coverage, as needed.

(b) Add or remove beneficiaries, or edit existing SGLI beneficiary information.

(c) View, save, print or email a SGLI Coverage Certificate.

(2) Ensure dependent information is updated within Defense Enrollment Eligibility Reporting System (DEERS.)

9-4. Timeline: Changes to beneficiaries, coverage increases, and restorations of coverage are effective immediately. Reductions to coverage amounts and coverage cancellations are not effective until the first day of the month following the date a member makes his/her election to reduce coverage amount or cancel coverage. Until that date passes, the member will continue to see the previous coverage amount.

9-5. References:

a. DoDI 1341.14, SGLI ON-LINE ENROLLMENT SYSTEM

b. Appendix A – References

Chapter 10
Real-time Automated Personnel Identification System (RAPIDS)

10-1. Overview: RAPIDS is a United States Department of Defense (DoD) system used to issue the definitive credential within DoD. RAPIDS uses information stored in the DoD Defense Enrollment Eligibility Reporting System (DEERS) when providing these credentials. Used together, these two systems are commonly referred to as a DEERS/RAPIDS system or DEERS/RAPIDS infrastructure.

10-2. Access: Permissions are determined based on the user's role and the recommendations from the Brigade.

a. Users must complete initial or annual certification training IAW Appendix G. The certification/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 a DD Form 2875 and DD Form 2841 annually. Email ng.ga.gaarng.list.g1-human-resource-systems@army.mil for the latest version of templates for each document.

10-3. Roles/ Responsibilities: Each Brigade S-1 Office is assigned a deployable machine. Each site must maintain two Site Security Managers (SSMs) and as many Verifying Officials (VOs) to accomplish their mission. Brigades coordinate among their Battalions to support DEERS support within their Brigades.

a. State Site Security Manager (SSM):

(1) Serves as liaison between the Brigades, State DEERS/RAPIDS sites, and NGB Service Project Office.

(2) Maintains access and process cases via IPPS-A CRM case.

(3) Conducts quarterly review of deployable sites, and address any unexplained or unresolved discrepancies with the site's SSM.

(4) Reviews and retains copy of site requests for training and verification of new SSMs and VOs.

(5) Schedules and conducts a minimum of one unannounced annual DEERS/RAPIDS site visit each calendar year.

(6) Monitors site activity 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. The roster will also include site number, city location, phone number, completed user training and date of current background investigation.

(8) Maintains a signed and dated copy of DD Form 2841, Public Key Infrastructure (PKI) Agreement for DEERS/RAPIDS users, on every SSM and Verifying Official (VO).

(9) Ensures distribution of updates, policy reviews and information to SSMs of each site.

(10) Perform all roles of the VO and Brigade SSM.

b. Brigade Site Security Manager:

(1) Maintains a signed and dated copy of DD Form 2841 (PKI Agreement for DEERS/RAPIDS Users) and proof of a NACI for each SSM and VO. 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 for transition.

(3) Ensures the Privacy Act Statement and DD Form 2842 are posted within workstations.

(4) Ensures all deployable RAPIDS systems are powered on and connected to VPN regularly to ensure that RAPIDS updates are received. Ensures all site users log onto the system at least once every thirty days to remain active and that they complete their annual recertification requirement.

(5) Ensures cardstock is accurate to the Inventory Logistics Portal (ILP,) and securely stored at the end of each business day. Ensures ALL CACs and USIDs that must be returned to DMDC are properly labeled in the front lower right corner.

(6) Returns expired/failed cardstock regardless of amount at least monthly, or more often if necessary, to the DMDC Support Center to ensure CACs are properly accounted for in the ILP. Check for ILP discrepancies at least monthly.

(7) Notifies the Chain of Command to initiate a 15-6 investigation when the cardstock discrepancy reaches 11 or more. The investigation must be completed within 45 calendar days of report of discrepancy.

(8) Ensures used printer ribbons are cross shredded to safeguard personal information.

(9) Performs all roles of the VO.

c. Verifying Official (VO):

(1) Must be a U.S. citizen and vetted in accordance with DoD 5200.2-R, meets the requirements for holding an IT-II position as described in DoD Directive 8500.1 (favorable NACI).

(2) Responsible for verification of identify of all Service Members and beneficiaries thru available supporting documentation. Updates records data and issues ID Cards.

(3) Must code all returned cards on the front lower right corner of the card.

10-4. References:

a. RAPIDS User Guide

b. Air Force Instruction 36-3026_IP Volume 1

c. Army Regulation 600-8-14

d. DoD 5200.2-R, PERSONNEL SECURITY PROGRAM

e. Appendix A – References

f. Appendix G – RAPIDS Access and Training

Appendix A
References

Section I
Publications

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 RECORD 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

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