Human Resources Systems Branch (NGGA-PES)

Human Resources Systems

Joint Force Headquarters
Georgia Army National Guard
Marietta, GA
15 October 2021

UNCLASSIFIED

Contents

Chapter 1
Introduction

1-1. Purpose: This Standing Operating Procedures (SOP) provides policies and procedures for Georgia Army National Guard's (GAARNG) Soldiers utilizing Human Resources(HR) Systems. This document covers access, managing, and updating personnel records via 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 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 under 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, leaders and Soldiers. Report fraud and forgery immediately to G-1 HR Systems via ng.ga.gaarng.list.g1-human-resource-systems@mail.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. GAARNG went live November 2019 with some functionally. IPPS-A will undergo another transformation September 2022 with Regular Army and Army Reserve joining the system. More functionally will come during the transformation, and once IPPS-A is fully deployed, the system will enable HR transactions to automatically trigger Soldier pay. In addition, Soldiers 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@mail.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.csd.disa.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 G-1.

(1) Enrollment into DL and IFT is managed by G-1 HR Plans Branch. Users will contact, through their MSC HR Tech (for users at MSC level or below) or Section OIC/NCOIC (for users at the state staff directorate), G-1 HR Plans Branch at ng.ga.gaarng.list.g1-hr-plans@mail.mil for enrollment. Once enrollment is confirmed, users will access IPPS-A at https://hr.ippsa.csd.disa.mil/ to complete DL, then attend IFT on the scheduled class dates.

(2) Once both DL and IFT are complete, users will log into IPPS-A at https://hr.ippsa.csd.disa.mil/ in order to request elevated user access. Access request may be submitted 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 will be automatically or manually de-provisioned in the event one of the following occurs.

(1) Automatic de-provisions;
(a) User receives re-assignment or transfer (PCA/TER/XFR)
(b) User does not log on for 90 consecutive days

(c) If user access need access restored, users must submit a new access request IAW paragraph 2-2a.

(2) Manually de-provisions;
(a) Users lose their security clearance level required IAW PPOM 18-040
(b) Users are found to have violated action IAW paragraph 2-4
(c) If user access need access restored, users must submit a new access request IAW paragraph 2-2a

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/manage Helpdesk cases, enroll and manage IPPS-A training, set enlisted promotion preference; 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 Resources 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) HR Professional Plus: This role allows all the HR Professional's access without requiring to workflow transactions within assignment module.

(4) Commander: Access to personnel actions, special pay 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, APFT), 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 an action and provide comments, review and comment on workflow requests, view and approve direct reports IPPS-A training.

(5) Manager: Access to view Members' dependent and beneficiary information, benefits enrollment, security clearance, duty status, emergency contact information, assignments, Soldier Record Brief, nine predefined queries, roster of members with P3 or P4 in their PULHES, talent profile, training summary, orders, position information, physical qualifications, deployment readiness, line of duty, military training, non person profiles Aviation, Job Code (MOS/MOSW/AOC), military education level, Physical Profiles (PULHES, APFT), Qualifications (PRP, ASVAB), Skills (SQI, ASI), etc. Additionally approve workflow requests, recommend approval or denial of an action and provide comments, review and comment on workflow requests.

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 catch 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 within HR Systems Branch. HR Systems branch will maintain the violations for one year and execute the following actions:

a. User's first violation will result in an email to the user's Brigade S-1 leadership.

b. User's second violation will result in access suspension 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 access suspension, 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 saved for future use. In order to maintain updated and relevant workflows, G-1 HR Systems Branch will provide a quarterly update of all current workflows to all HR Professionals within IPPS-A. Although HR Systems will update the shared workflows quarterly, in order for users to utilize templates, users must save the templates within their profile.

a. Add workflow tile to homepage:

(1) From the HR Professional Homepage type "Workflow save as" in the global search engine.

(2) Select "Workflow Save As Preference".

(3) Add to homepage by selecting the three dot icon on the top right of screen within

IPPS-A

b. Saving updated workflows:
(1) Within, *Workflow Save As Preference* page, select radio box next to "Shared Templates"
(2) Type the name of the template provided and click search.
(3) Select the details next to each description box. This will open up on another tab.
(4) Select Import Template. Select Ok. Close the tab.

c. Removing old Workflows:
(1) Within, *Workflow Save As Preference* page, under "workflow template"
(2) Click the trash can icon next to the template to remove

d. Request update or creation of workflows by submitting a request to HR Systems Branch via admin correction PAR within IPPS-A or email request to ng.ga.gaarng.list.g1-human-resource-systems@mail.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 admin correction PAR within IPPS-A or email request to ng.ga.gaarng.list.g1-human-resource-systems@mail.mil

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

a. State HR Systems Branch:
(1) Manage access within IPPS-A
(2) Provide IPPS-A Support (Appendix B)
(3) Conduct quarterly training for new users
(4) Manage all entry active duty (EADT) transitions
(5) Conduct weekly audits IAW Internal Control Compliance Guide
(6) Provide a monthly report of user access/PAR workflows/S1 pools

b. State Human Resource Office:
(1) Manage actions required for Active Guard Reserve (AGR) Soldiers.
(2) Manage actions required for Title 32 Technicians

c. Brigade S-1 Office:
(1) Process actions IAW this SOP
(2) Monthly review of user access/PAR workflows/S1 pools, within their Brigade
(3) Maintain actions process for Brigade and below transactions

d. Battalion S-1 Office:
(1) Process actions IAW this SOP
(2) Monitor and process all actions within S-1 Pool

e. Soldiers:
(1) Review and update personnel data
(2) Notify unit chain of command of data discrepancies

2-8. References:

a. IPPS-A ARNG User Manual, Provided by 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@mail.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/rms/login-paa

b. Requirements for additional 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 role(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@mail.mil.

e. Domain Administrators will only assign user role or rule IAW Appendix C. For any and all exception that is not specifically addressed in Appendix C (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 E.

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.

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 financial and personnel record audits.

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: An individual Soldier can view and download their 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) Manage DM\DA Access
   (2) Process 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
   (3) Process all accession iPERMS batches

b. Brigade S-1:
   (1) Manage access IAW Appendix E
   (2) Verify and process all batches from subordinate battalions and units
   (3) Process all batches in the Brigade QC role
   (4) Ensure subordinate units and battalions are completing all required iPERMS actions

c. Battalion S-1:
   (1) Process all batches in the battalion Personnel Services Specialist's designated roles on a consistent basis

(2) Verify all batches from subordinate units
(3) Ensure records management is taking place in all subordinate units
(4) Receive and review iPERMS user requests, ensuring completeness prior to forwarding to Brigade
(5) Forward all approved requests for access to the Brigade Personnel Services Specialists

d. Unit Personnel:
(1) Scan and Index all documents created at the unit level into iPERMS
(2) Give Soldiers the opportunity to an annual records review, and ensure all updated documents are then scanned and indexed into iPERMS
(3) All documents in the Soldier's AMHRR that do not belong to that Soldier, use the "Report a Problem" tool for document corrections

3-5. 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/RECORDS
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

Chapter 4
SIDPERS Interface Branch-X (SIBX Web)

4-1. Overview: SIBX used to provide live SIDPERS data access to the end unit through a user-friendly graphical interface. This application consolidates data from SIDPERS, RCAS, AFCOS, ATRRS, and other sources to create a comprehensive “one stop shop” with numerous benefits. Since going live with IPPS-A, SIBX is a tool GAARNG users needs to use with understanding the data may not be accurate. IPPS-A is the database of record for personnel data.

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. Exemptions to this rule are Administrative Officers, Executive Officers, S1, HR Technicians and NCOICs, as they are authorized high headquarters access within SIBX.

a. SIBX can be accessed at https://webpr-ga.ng.ds.army.mil:8890/ords/f?p=104:101

b. Submit DD Form 2875 IAW Appendix C annually to G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@mail.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 SIBX.

4-4. References:

a. SIBX User Guide
b. Appendix A – References

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 pulls information from dozens of primary data sources.

5-2. Access: Permissions are determined based on the user's role and command hierarchy level. Request 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 within the online request, request above State level will not be seen within Georgia)
d. Attach completed DD Form 2875, IAW Appendix C

5-3. Functions/Features: The following describes the common functions and features accessible within DPRO, more detailed list 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 accessible to all DPRO users. These reports provide you 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 you with the ability to quickly see how the value of key metrics has changed over a time-frame of your choosing.

e. Search Function: With the embedded search engine, found on the far-right end of the DPRO Ribbon Toolbar, you can search throughout DPRO for 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 your enterprise email account.
(1) Daily subscriptions are sent out every day between 8 p.m. and 6 a.m.
(2) Weekly subscriptions are sent Monday through Friday between 6 p.m. and 6 a.m. (Monday's subscription email contains Friday data). 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 to the users beginning the first of each month and continue until all subscriptions are sent (meaning some users may receive their subscription on the second or third 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 out.

5-4. References: Web-friendly user guide within DPRO, the Help menu in the Ribbon Toolbar, click User Guide.

Chapter 6
Record Brief

6-1. Overview: The Record Brief application is an administrator's interface for Human Resource Specialist within the Army National Guard to review and update the Record Briefs of other Soldiers within their Unit or State.

6-2. Access: Permissions are determined based on the user's role and command hierarchy level. Request 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 within the online request, request above State level will not be seen within Georgia)
d. Attach completed DD Form 2875, IAW Appendix C

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

a. View Record Brief: Users assigned this role can view record briefs for Soldiers in their assigned command hierarchy. This is the role most Record Brief users are assigned.
b. Edit Record Brief: Users assigned this role can edit record brief content for Soldiers in their assigned command hierarchy.
c. Super Editor: Users assigned this role can edit record brief content for Soldiers in their assigned command hierarchy. They may also be given the permissions to manage other user's access to Record Brief.
d. Admin: Users assigned this role edit Record Brief content and manage other user's access 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 link.
b. Validated Record Brief: reviewed by the Soldier and has verified that everything is accurate. After the Record Brief has been validated, the potential exists for the Record Brief and Validated Record Brief files contain different data. This is because once the Record Brief has been validated, a snapshot of the data is taken at that point in time and saved within the system. 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: user agreed that he/she has reviewed the Soldier's Record Brief for accuracy and is certified all information contained within it is correct. While the ideal progression is for the Record Brief to be certified after it has been validated by the Soldier, the Unit can certify a Record Brief that has not previously been validated, so the Record Brief to be shown before a Board.
d. Selection Board Record Brief: mimics what a Board sees on a Soldier's Record Brief though it has certain Personal Information redacted.

6-5. Responsibilities:

a. G-1 HR Systems Branch:
   (1) Manage user access

b. Brigade S-1:
   (1) Ensure subordinate commands are following this SOP and guidance via user manual

c. Battalion S-1:
   (1) Provide units/Soldiers with an annual records brief
   (2) Update required authority data base of record IOT update Soldier's data

d. Soldier:
   (1) Record Briefs must be validated by the individual Soldier via the benefits site using the URL https://arngg1.ngb.army.mil/SelfService/CareerCenter. They cannot be validated through the Record Brief Application

6-6. References: Record Brief User Guide, found within Record Brief.

Chapter 7
Mission Personnel Accountability System (MPAS)

7-1. Overview: MPAS is a state system used to maintain accountability of personnel on missions for state active duty. During State Active Duty (SAD) missions, Brigades report through MPAS their daily Personnel Status Report (PERSTAT).

7-2. Access: Any Georgia Domain user can access MPAS.

a. User must be logged into the Georgia Network/ domain at https://ga-nec/mpas/.
b. Access to edit personnel on mission is determined each mission.
c. Access is based on command hierarchy level and need to know.

7-3. Responsibilities: G-1 HR Plans manages the CONPLAN for responding to SAD missions and the reporting requirements within MPAS.

7-4. References: Follow guidance within CONPLAN 3500 Anx E (Personnel)

Chapter 8
Reserve Component Automation Systems (RCAS)

8-1. Overview: The Reserve Component Automation Systems (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), Integrated Personnel and Pay System - Army (IPPS-A) program office and is the Army proponent for RCAS. RCAS provides a modernized system for performing your day-to-day jobs as well as new functionality.

8-2. 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 submit completed DD Form 2875, annually to G-1 HR Systems Branch at ng.ga.gaarng.list.g1-human-resource-systems@mail.mil through MSC HR Tech (for users at MSC level or below) or Section OIC/NCOIC (for users at state staff directorate)
c. All access to RCAS users are required to register their CAC with AKO.

8-3. Roles: Within GAARNG, there are three main roles utilized within RCAS.

a. Retirement Points Accounting Management - Next Generation (RPAMNext): A web-based application that creates and updates RPA records for members of the Army National Guard. Primary application functions include the following and is managed by G-1 HR Services Section:
(1) Enabling RPAM Administrators to maintain the retirement point accounts of individual Soldiers.
(2) Qualifying Soldiers for non-regular retirement.
(3) Importing and validating data from outside databases such as IPPS-A.
(4) Importing and exporting data to/from other states for Soldiers who move from one state to another.
(5) Generating more than 20 various reports and form letters, including NGB Forms 23A, 23A1, 23B, 23C, 23D, 23E, and 23F.
(6) Calculating eligibility for Early Retirement Pay (ERP), and calculating and displaying the Retirement Pay Eligibility Date (RPED) for Soldiers (including Forms 23A, 23B, and 23C).

b. Mobilization Planning Data Viewer (MPDV): provides a seamless interface across the information systems required to support mobilization planning and is managed by G-1 HR Plans Section.

c. Safety and Occupational Health (SOH): supports both the ARNG and the USAR in complying with Army safety requirements and regulations. SOH is a web-based application that provides an automated system for collecting, recording, and reporting data on occupational health and safety matters. SOH provides data collection for:
(1) Accident investigation and reporting
(2) Inspection scheduling and management
(3) Hazards identification and abatement
(4) System defect or inadequacy review and management
(5) Hazard analysis to create system defects
(6) Safety training planning and management

(7) Safety Orders
(8) Individual and unit safety awards
(9) Radioactive item inventory management.

8-4. 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

Chapter 9
Electronic Military Personnel Office (eMILPO)

9-1. Overview: eMILPO application is primarily used for Active Army's personnel database and is accessible 24/7 worldwide. The Army National Guard uses eMILPO to manage the DD Form 93, Record of Emergency Data. eMILPO allows users to input data to create the DD Form 93 for a new accession or a Soldier requiring an update to their DD Form 93. This function also allows the DD Form 93 to be digitally signed and automatically uploaded to iPERMS. The DD Form 93, when completed and signed, becomes an official and legal document that designates the beneficiaries of certain benefits in the event the individual is in a missing status or deceased. The DD Form 93 provides the names and addresses of the person(s) to be notified in case of an emergency, sickness or death

9-2. Access: Permissions are determined based on the user's role and command hierarchy level.

a. System can be accessed at https://emilpo.ahrs.army.mil/
b. Failure to log into eMILPO within 30 days results in an automatically locked account, contact your MSC HR Tech (for users at MSC level or below) or Section OIC/NCOIC (for users at state staff directorate).
c. Submit DD Form 2875 (Appendix C) annually MSC HR Tech (for users at MSC level or below) or Section OIC/NCOIC (for users at state staff directorate).

9-3. Responsibilities: DD Form 93 are to be updated annually or when needed. The following sections or individuals are responsible for the information listed below.

a. Brigade S-1 MSC Tech and NCOIC:
   (1) Manage access within their Brigade
   (2) Maintain required annual SAARs for accountability
   (3) Ensure Battalions are trained on the proper completion of the DD Form 93
   (4) Develop a plan to maintain 80% completion of annual requirement

b. Battalion S-1 Office:
   (1) Update Soldier's DD Form 93
   (2) Maintain a digital record to ensure iPERMS updates within 5 business days
   (3) Educate Soldiers on the requirements for a DD Form 93

c. Soldiers:
   (1) Notify chain of command when updates are required outside annual requirement

9-4. References:

a. Appendix A – References
b. Appendix F – DD Form 93 Example

Chapter 10
SGLI Online Enrollment System (SOES)

10-1. 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 (Figure 10-1). SOES centralizes SGLI/FSGLI data into one authoritative system capable of providing consistent SGLI/FSGLI information to members and their leadership.

10-2. 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 using Internet Explorer at www.dmdc.osd.mil/milconnect.
b. To see and update SGLI, 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.

10-3. Responsibilities: SGLI are to be updated annually or when needed. The following sections or individuals are responsible for the information listed below.

a. Battalion S-1 Office:
   (1) Track and notify Soldiers requiring updated SGLI
   (2) Develop a plan to maintain 80% updated throughout the fiscal year
   (3) Educate Soldiers on the requirements for a SGLI

b. Soldiers:
   (1) Update their annual SGLI or updated as needed. Actions include but not limited to:
      (a) Increase, reduce or cancel SGLI and FSGLI coverage, as needed.
      (b) Add a beneficiary or edit SGLI beneficiary information
      (c) View, save, print or email a SGLI Coverage Certificate
   (2) Ensure dependent information is updated within DEERS.

10-4. 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 request. Until that date passes, the member will continue to see the previous coverage amount.

10-5. References:

a. DoD 1341.14, SGLI ON-LINE ENROLLMENT SYSTEM
b. Appendix A – References

Chapter 11
Real-time Automated Personnel Identification System (RAPIDS)

11-1. 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.

11-2. Access: Permissions are determined based on the user's role and Brigade recommendations. Each site must maintain at least two Site Security Managers.

a. Users must complete training annually within Joint Knowledge Online Learning Management System IAW Appendix G.
b. Once certification or re-certification has been complete, users must complete a DD Form 2875 and DD Form 2841 annually. Email ng.ga.gaarng.list.g1-human-resource-systems@mail.mil for the latest version templates.

11-3. Roles/ Responsibilities: Each Brigade S-1 Office is assigned a deployable machine. Each site must maintain two Site Security Manager (SSM) 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) Serve as liaison between the Brigades, NGB and State DEERS/RAPIDS sites.
   (2) Maintain access and process cases through eTracker
   (3) Conduct quarterly review of deployable sites and address any unexplained/unresolved discrepancies with the site's SSM.
   (4) Review and retain copy of site requests for training and verification of new SSMs and VOs.
   (5) Schedule and conduct a minimum of one unannounced annual DEERS/RAPIDS site visit at each site.
   (6) Monitor site activity to ensure all users are logging in and utilizing the systems at least once a month.
   (7) Maintain 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) Maintain 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) Ensure distribution of NGB 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) Maintain 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. Provide copies to the STATE SSM.
   (2) Notify State SSM immediately of any pending SSM or VO personnel change and the site's plan for transition.
   (3) Ensure the Privacy Act Statement and DD Form 2842 are posted within workstations.

(4) Ensure all deployable RAPIDS systems are powered on and VPN connected regularly to ensure that RAPIDS updates are received. Ensure 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) Ensure cardstock is accurate to the ILP and locked up at the end of each day. Ensure ALL CACs that must be returned to DMDC are coded on the front, in the lower right corner.
(6) Return 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 Inventory Logistics Portal (ILP). Check for ILP discrepancies at least monthly.
(7) If your cardstock discrepancy is 11 or more, you are required to have your Chain of Command initiate a 15-6 investigation. The investigation must be completed within 45 calendar days of report of discrepancy.
(8) Ensure used printer ribbons are cross shredded to safeguard personal information.
(9) Perform 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 thru certain supporting documentation of all Service Members and beneficiaries. Update records data and issue ID Cards.
(3) Must code all returned cards on the front right bottom of the card.

11-4. 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

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)

DA Form 93
RECORD OF EMERGENCY DATA

Abbreviations

AGR
Active Guard/Reserve

AMHRR
Army Military Human Resource Record

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

DEERS
Defense Enrollment Eligibility Reporting System

DMDC
Defense Manpower Data Center

DoD
Department of Defense

DPRO
Directors Personnel Readiness Overview

DL
Distance Learning

DSC
DMDC Support Center

eMILPO
Electronic Military Personnel Office

HR
Human Resource

IFT
Instructor Facilitated Training

IPPS-A
Integrated Personnel and Pay System - Army

iPERMS
Interactive Personnel Electronic Records Management System

MPAS
Mission Personnel Accountability System

MSC
Major subordinate command

NGB
National Guard Bureau

RAPIDS
Real-time Automated Personnel Identification System

RCAS
Reserve Component Automation Systems

SAAR
System Authorization Access Request

SIDPERS
Standard Installation/Division Personnel System

SGLI
Servicemembers' Group Life Insurance

SSM
Site Security Manager

SOES
SGLI Online Enrollment System

VO
Verifying Official