Human Resource Systems
(NGGA-PEP-SYS)

Systems Access

Joint Force Headquarters
Georgia Army National Guard
Marietta, GA
1 October 2018
SUMMARY of CHANGE

SOP 4-1
System Access

- No changes. First edition, 1 October 2018.

Proposed changes, modifications, and/or deletions should be made known GAARNG G-1, HR Plans using GA Form 2028.
Your feedback to provide a quality product is always welcome.
## Contents

**Chapter 1 Overview**
- 1-1 Purpose
- 1-2 References
- 1-3 Scope

**Chapter 2 Requesting System Access**
- 2-1 Overview
- 2-2 Requirements
- 2-3 Access Suspension or Removal
- 2-4 Standard Installation/Division Personnel System Army National Guard (SIDPERS-ARNG)
- 2-5 SIDPERS Interface Branch (SIBX)
- 2-6 Interactive Personnel Electronic Records Management System (iPERMS)
- 2-7 Reserve Component Automation Systems (RCAS)
- 2-8 DPRO/Record Brief (RB)
- 2-9 Electronic Military Personnel Office (eMILPO)
- 2-10 Security Clearance Requirement
- 2-11 Network

**Chapter 3 DD Form 2875, System Authorization Access Request (SAAR)**
- 3-1 Overview
- 3-2 Initial SIDPERS Access
- 3-3 G1 System DD 2875

**Chapter 4 Personally Identifiable Information (PII)**
- 4-1 Overview
- 4-2 PII Breach

**Appendix A**

References

Glossary
Chapter 1 - Overview

1-1 Purpose

Georgia Army National Guard (GAARNG) Human Resource System (HRS) Access provides access to all personnel systems managed by Georgia. The G1-HRS Branch is responsible for overseeing access to the following systems which all have their individual SOPs for reference:

- Standard Installation/Division Personnel System Army National Guard (SIDPERS-ARNG)
- SIDPERS Interface Branch (SIBX)
- Interactive Personnel Electronic Records Management System (iPERMS)
- Reserve Component Automation Systems (RCAS)
- Record Brief
- Directors Personnel Readiness Overview (DPRO)
- Electronic Military Personnel Office (eMILPO)

1-2 References

See Appendix A

1-3 Scope

All personnel employed to support the administrative functions in the Georgia Army National Guard (GAARNG) will adhere to policies and procedures set forth herein. Additionally, all personnel will conform to accept procedures and standards as published or implied in technician personnel, National Guard or Army directives.
Chapter 2 - Requesting System Access

2-1 Overview

Human Resource Systems (HRS) section manages the process below for requesting access to the following subsections of personnel systems. HRS assigns a system administrator within the HRS section to coordinate with each MSC HR Technician to manage their MSC’s access process and requirements. All users will route access related issues through the MSC’s HR Technicians.

2-2 Requirements

All systems require a DD Form 2875, see Chapter 3 for completion instructions for submitting DD Form 2875. A fillable DD Form 2875 can be obtained from http://www.apd.army.mil/. Users will complete the DD Form 2875 and forward to the appropriate levels mentioned in the subsections below.

All users will maintain a minimum interim SECRET security clearance

Users must have a valid DoD Cyber Awareness Challenge Training Certificate when submitting for access using the DD Form 2875. The DoD Cyber Awareness Challenge Training Certificate is valid for one year: https://cs.signal.army.mil/DoDIAA/default.asp

It is the user’s responsibility to submit a new form prior to the anniversary date of their last DD 2875.

New or extended access requires 72 hours processing time upon receipt in the HRS Section. Do not contact HRS Section directly unless DD 2875 has been received and 72 hours have elapsed.

2-3 Access Suspension or Removal

Access will be removed or suspended upon expiration of latest DD 2875. To prevent loss of access annual DD 2875s should be processed 30 days prior to expiration.

If, at the discretion of the HRS OIC or NCOIC, a user is determined to have knowingly committed an erroneous transaction their access will be suspended for a timeframe determined by the HRS OIC or NCOIC. MSC’s HR Technicians can communicate when or if they want their Soldier’s access reinstated.

When a user no longer requires access, the MSC’s HR Technicians, OIC or NCOIC will immediately submit a request to deactivate the user’s account to ng.ga.gaargn.list.g1-human-resource-systems@mail.mil.

2-4 Standard Installation/Division Personnel System Army National Guard (SIDPERS-ARNG)

SIDPERS access requests requires a “SIDPERS” DD 2875 found in section 3-2. SIDPERS accounts are managed by HRS.

All SIDPERS access requires an initial training course, given by HRS section quarterly. MSC’s HR Technicians will coordinate with HRS section to enroll their users for initial access training.

Level of access or group is determined by the position the user holds and can be found within HRS’s SIDPERS SOP.

A new DD 2875 is required when a user changes positions to determine the new level of access.

2-5 SIDPERS Interface Branch (SIBX)

SIBX Access requires the “G1 System Access” DD 2875 found in section 3-3. SIBX accounts are managed by HRS.

Level of access or group is determined by the position the user holds and can be found within HRS’s SIBX SOP.

A new DD 2875 is required when a user changes positions to determine the new level of access.

Access to see General Officers is a separate level added to the DD Form 2875, and will only be approved by G1 or Deputy G1.
2-6 Interactive Personnel Electronic Records Management System (iPERMS)

iPERMS Access requires the “G1 System Access” DD 2875 found in section 3-3. iPERMS accounts are managed by the Domain Administrators or Manager for JFHQ.

The State iPERMS Domain Manager within the HRS section will control all Domain Administrators’ (DA) accounts. The DAs, typically the MSC HR Technicians, will manage all accounts within their organizations.

Determination for access will be made IAW AR 600-8-104, Chapter 2, Access to the Interactive Personnel Electronic Records Management System.

iPERMS access requires annual training using the web-based training at https://ipermstraining.carson.army.mil/wbt/.

Only the State iPERMS Domain Manager can approve requests for “statewide” access.

Only the G1 or Deputy G1 may approve requests for access to General Officers’ records.

See HRS iPERMS SOP for more detail.

2-7 Reserve Component Automation Systems (RCAS)

RCAS Access requires the “G1 System Access” DD 2875 found in section 3-3. RCAS accounts are managed by HRS.

To receive initial access, users must login https://nggac2-app01.ng.ds.army.mil/RCASWeb and “Request Access” in the upper right hand corner of the website.

All access to RCAS users are required to register their CAC with AKO.

Publishing rights and levels of access is determined by the position the user is assigned, see HRS RCAS SOP for more details.

2-8 DPRO/Record Brief (RB)

DPRO Access requires the “G1 System Access” DD 2875 found in section 3-3. DPRO access is required IOT be granted a RB account, which is managed by HRS.

The DD 2875 must be uploaded in the DPRO website and request for access must be done to receive initial access. Users will login https://arngg1.ngb.army.mil/Portal/Default.aspx and “Request Access” in the upper left portion of the website.

All access to DPRO/RB requires users to register their CAC with AKO.

Levels of access is determined by the position the user is assigned.

2-9 Electronic Military Personnel Office (eMILPO)

eMILPO Access requires the “G1 System Access” DD 2875 found in section 3-3. eMILPO accounts are managed by the MSC HR Technicians.

Accounts must be logged into within 30 days or the users will be locked.

See HRS eMILPO for more details.

2-10 Security Clearance Requirement

All DSIB/SIDPERS users will maintain a minimum interim SECRET security clearance.
2-11 Network

All personnel systems will take place over the Georgia National Guard Domain Network. Users will use the following links below to access systems.

a. Standard Installation/Division Personnel System Army National Guard (SIDPERS-ARNG)
   i. Non CAC Link: https://nggaa0u1.ng.ds.army.mil:8890/forms/frmservlet?config=sidpers
   ii. CAC Enabled Link: https://nggaa0u1.ng.ds.army.mil:8890/forms/frmservlet?config=sidpers_cac

b. SIDPERS Interface Branch (SIBX)

   c. Interactive Personnel Electronic Records Management System (iPERMS)
      i. GA Domain Link: https://iperms-ga.hrc.army.mil/rms/
      ii. DoD Link: https://iperms.hrc.army.mil/rms/login-paa

d. Reserve Component Automation Systems (RCAS)
   i. Link: https://nggac2-app01.ng.ds.army.mil/RCASWeb

e. Directors Personnel Readiness Overview (DPRO) / Record Brief
   ii. Application Link: https://armgg1.ngb.army.mil/Portal/

f. Electronic Military Personnel Office (eMILPO)
   i. Link: https://emilpo.ahrs.army.mil/
Chapter 3 - DD Form 2875, System Authorization Access Request (SAAR)

3-1 Overview

The DD 2875 is used to record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. The SAAR application must be digitally signed to validate Soldiers’ authenticity.

3-2 Initial SIDPERS Access

For access to SIDPERS, a separate DD 2875 is required.

Users must follow the following steps:

a. Place an "X" in the initial block with the “Type of Request” section
b. Add “GA SIDPERS” as the system name
c. Complete part 1 as described on the instruction page of the DD 2875
d. Block 13 requires the assigned position of the user to identify the level of SIDPERS they will receive IAW HRS SIDPERS SOP
  e. The supervisor will verify block 16 by placing an “X” and completing the remainder of part II IAW the instruction page 2 of the DD 2875
f. Block 21 through 25 will remain blank until processed through the Systems Administrator
g. Block 27 needs to explain which UICs the Soldier needs access to
h. Part III will be completed by a security manager within each MSC IAW the instruction page
i. MSC HR Technicians will forward the SAARs to mailto:ng.ga.gaarng.list.g1-human-resource-systems@mail.mil
j. See Figure 3-1 for the example of the user and supervisor’s part (part I and II) of the DD 2875 for the GA SIDPERS

3-3 G1 System DD 2875

Access to all the G1 managed systems mentioned in Chapter 2, one annually completed G1 System DD 2875 is required.

Users must follow the following steps:

a. Place an “X” in the initial block with the “Type of Request” section
b. Add “GA G1 Systems: SIBX, RCAS, iPERMS, SMMS SUITE(DPRO/Record Brief), eMILPO” as the system name
c. Complete part 1 as described on the instruction page of the DD 2875
d. Block 13 requires the assigned position, job description, and brief statement explaining why the user needs to have access
e. The supervisor will verify block 16 by placing an “X” and completing the remainder of part II IAW the instruction page 2 of the DD 2875
f. Block 21 through 25 will remain blank until processed through the Systems Administrator
g. Part III will be completed by a security manager within each MSC IAW the instruction page
h. Block 27 needs to explain which UICs the Soldier needs access to
i. MSC HR Technicians will forward the SAARs to mailto:ng.ga.gaarng.list.g1-human-resource-systems@mail.mil
j. See Figure 3-2 for the example of the user and supervisor’s parts (part I and II) of the DD 2875 for the GA G1 Systems
Figure 3-1: Template of the user and supervisor parts of DD 2875 for GA SIDPERS
Figure 3-2: Template of the user and supervisor parts of DD 2875 for GA G1 Systems
Chapter 4 - Personally Identifiable Information (PII)

4-1 Overview

Personally Identifiable Information (PII) is any information about an individual which can be used to distinguish or trace an individual's identity such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, and biometric records. This information can be in hard copy (paper copy files) or electronic format, stored on personal computers, laptops and personal electronic devices such as BlackBerry® devices and found within databases. This includes but is not limited to, education records, financial transactions, medical files, criminal records, or employment history.

As an individual, you have rights regarding:

a. What information is collected about you
b. How it will be used
c. The ability to correct it if necessary
d. Having it protected from unauthorized disclosure

As an Army employee (civilian, military) or contractor, you have responsibilities to:

a. Be able to recognize PII and safeguard it
b. Collect PII only when authorized
c. Collect only necessary information
d. Tell the individual why you are collecting PII, who will see it, and what will happen if the individual does not provide the requested information
e. Keep the PII accurate, relevant, timely and complete
f. Keep PII confidential and protect it from misuse or loss or breach

4-2 PII Breach

Breaches often occur when PII or Personal Health Information (PHI) is mishandled.

Examples of these types of breaches may include, but are not limited to:

a. Posting PII on public websites
b. Sending PII via email to unauthorized recipients
c. Transmitting unsecured emails and unencrypted files containing PII
d. Providing hard copies containing PII to individuals without a need to know
e. Failing to properly secure documents containing PII when mailing or transporting
f. Misdirected fax documents containing PII that reach anyone other than the intended recipient
g. Lost or stolen electronic devices or media storing PII (e.g., laptop, BlackBerry®, CD, or flash-based storage media)
h. Successful network intrusions
i. Unauthorized access to computer systems
j. Inappropriate disposal of documents containing PII
k. PII use by employees for unofficial business
l. Unauthorized access to credit card information
m. Loss or unauthorized access to PII (including a temporary loss of control)

Examples of this type of breach include:

n. Anytime persons gain access to PII without an official need-to-know on intra-agency websites and through bulletin boards in common areas

All other unauthorized access to PII.

Appendix A

References

Forms

DD Form 2875
System Authorization Access Request

Glossary

Abbreviations

AGR
Active Guard/Reserve

AMHRR
Army Military Human Resource Record

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

CAC
Common Access Card

DA
Domain Administrator

DM
Domain Manager

DPRO
Directors Personnel Readiness Overview

DSIB
Decentralized SIDPERS

eMILPO
Electronic Military Personnel Office

ETS
Expiration Term of Service

GO
General Officer

iPERMS
Interactive Personnel Electronic Records Management System

MSC
Major Subordinate Command

PHI
Personal Health Information

PII
Personally Identifiable Information
RCAS
Reserve Component Automation Systems

SAAR
System Authorization Access Request

SIBX
SIDPERS Interface Branch

SIDPERS
Standard Installation/Division Personnel Reporting System

TAG
The Adjutant General

UIC
Unit Identification Code