PRIVACY IMPACT ASSESSMENT (PIA)

For the

Global Combat Supply Support (GCSS) -Army
HQDA G4 - PEO EIS

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☐ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☒ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 621 (DA 01333)
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 007-21-06-01-5070-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0710-2b DALO

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 3013, Secretary of the Army; 42 U.S.C. 10606; DoD Instruction 1030.1, Victim and Witness Assistance; Army Regulation 600-8-104, Military Personnel Information Management/Records; and E.O. 9397 (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

GCSS-Army is the tactical unit / installation logistics and financial system for the U.S. Army. GCSS-Army is an Enterprise Resource Planning (ERP) solution that will track supplies, spare parts and organizational equipment. It will track unit maintenance, total cost of ownership and other financial transactions related to logistics for all Army units. This modernized application will subsume outdated Standard Army Management Information Systems (STAMIS) that are not financially compliant and integrate multiple supply and logistics databases into a single, enterprise-wide authoritative system. GCSS-Army will be financially compliant and is a key component for the Army Enterprise strategy to be financially auditable by the end of FY17. When fully deployed, GCSS-Army will affect every supply room, motor pool, direct support repair shop, warehouse and property book office in the Army, improving efficiency and visibility for 154,000 users.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The main privacy risk is exposure of personal information to unauthorized individuals or release of social security number.

GCSS-Army has significant safeguards built in to the system to protect PII. Subject matter experts conducted extensive analysis in developing user roles. Role-based user accounts ensure that only users with a valid business need have access to PII and that no user has access to information that is not required for their roles and duties. Data in transit across the network is protected by Secure Sockets Layer (SSL) or secure file transfer protocol (SFTP) encryption, using DOD Class 3 or 4 Public Key Infrastructure (PKI) certificates.

System access to PII is audited for both authorized and unauthorized access.

In addition, privileged and unprivileged users must undergo DOD and Army approved training for safely handling PII.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Department of the Army, Human Resources Command, Army Reserve Command, Army National Guard, Army Enterprise Systems Integration Program (AESIP), Defense Enrollment Eligibility Reporting System (DEERS), Electronic Military Personnel Office (EMILPO), and Army Civilian Personnel System (ACPERS)

☒ **Other DoD Components.**

Specify. U.S. Military Entrance Processing Command

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Northrop Grumman Mission Systems (NGMS) contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentially and security of a Soldier's PII. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of a work day. Contractual language directs and requires each NGMS employee in support of GCSS-Army to have a valid Secret clearance prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U.S. Code Section 522a, and all applicable agency rules and regulations.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

GCSS-Army will collect the individual's PII data from the source systems of eMILPO and DEERS directly interfacing with them only under some exceptional circumstances wherein the individual's information does not already reside in a source system of record. At this time, GCSS-Army support team will enter the PII data into system manually where an individual has the opportunity to consent based on the Privacy Act statement.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

GCSS-Army will collect the individual's PII data from the source systems of eMILPO and DEERS directly interfacing with them only under some exceptional circumstances wherein the individual's information does not already reside in a source system of record. At this time, GCSS-Army support team will enter the PII data into system manually where an individual has the opportunity to consent to specific use of PII based on the Privacy Act statement.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

GCSS-Army representatives will not request PII data directly from individual users of this system. GCSS-Army will collect PII directly from individuals only under exceptional circumstances when their information does not already exist in a source system of record.

The only direct point of PII data collection will be either retrieved electronically from an existing authoritative source, or will be collected by the user's local personnel representative (S1 or equivalent).

The Privacy Act Statement is directly from the standard DD 2875 form that a user fills out when requesting access to the GCSS-Army system:

PRIVACY ACT STATEMENT
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: 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. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.