



PRIVACY IMPACT ASSESSMENT (PIA)

For the

General Fund Enterprise Business System (GFEBS)

Program Executive Office Enterprise Information Systems & Assistant Secretary of the
Army (Financial Management & Comptroller) ASA (EM&C)

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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

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

0314

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.

GFEBs will be using both SORNs for this system.

The information contained in GFEBs is collected under the authority of Army & DoD CFOs.

5 U.S.C. 301 Departmental Regulation; Department of Defense Financial Management Regulation (DODFMR) 7000.14-R, Volume 5; 31 U.S.C. Sections 3511, 3512, and 3513; and E.O. 9397 (SSN).

5 U.S.C. 301, Departmental Regulations; 31 U.S.C. Chapters 37 and 39, Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 10; 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.

The General Fund Enterprise Business System (GFEBS) is the Army's web-based Enterprise Resource Planning (ERP) system, integrating financial, real property, cost management and performance data into one system. General Fund Enterprise Business System (GFEBS) is a decision support tool providing visibility of transactions across the Army, enabling well-informed business decisions at every organizational level for all three Army Components (Active Army, Army National Guard, and Army Reserve). General Fund Enterprise Business System (GFEBS) will transform the way the Army does business by enhancing the information available for decision making by Army leaders and managers. With over 79,000 end-users at more than 200 Army financial centers around the world, General Fund Enterprise Business System (GFEBS) will be one of the World's largest enterprise financial systems, managing around \$140 billion in spending by the Army Components. Army decision makers will be able to better leverage current resources and plan for future requirements.

General Fund Enterprise Business System (GFEBS) brings the majority of Army financial and real property management processes into a single system, allowing the Army to fully assess performance and costs, empowering leaders at all levels to determine the true costs of operations and the costs that affect their budgets. General Fund Enterprise Business System (GFEBS) will subsume over 80 legacy systems including the Standard Finance System (STANFINS) - the most widely used standard accounting system for Army installations, and the Standard Operation and Maintenance Army Research and Development System (SOMARDS). After implementation, General Fund Enterprise Business System (GFEBS) will be one of the world's largest government Enterprise Resource Planning (ERP) systems. General Fund Enterprise Business System (GFEBS) capabilities enable decision-makers to capitalize on current resources with enhanced functionality to determine and justify resource demands in support of the Warfighter. The goals:

- Provide decision support information to sustain Army Warfighting capability
- Furnish analytic data and tools to support Institutional Adaptation
- Reduce the cost of business operations
- Improve accountability and stewardship

General Fund Enterprise Business System (GFEBS) will move the Army from a "spend and consume culture" to a "cost and control culture" creating benefits for Congress, DOD, and Army Leadership, the Soldier, and the financial management community within the Army. The type of PII collected is personal, financial, employment, and military information.

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

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus the Program Executive Office Enterprise Information Systems & Assistant Secretary of the Army (Financial Management & Comptroller) ASA (FM&C) has determined the risk to the individual's privacy to be minimal.

Before General Fund Enterprise Business System (GFEBS) access is granted, users must be created and assigned roles in the SAP system user master records. A user can only log on to the system if he or she has a user master record. A user menu and data record authorizations are also assigned to the user master record via one or more roles. Roles are collections of activities which allow a user to use one or more business scenarios of an organization. The transactions, reports and Web-based applications defined in the roles are accessed using user menus. User menus should only contain the typical functions in the daily work of a particular user. The integrity of business data is also ensured by the assignment of roles. Authorization profiles are generated which restrict the activities of users

in the SAP System.

The General Fund Enterprise Business System (GFEBs) system will be certified and accredited according to the DIACAP. In addition, the certification and accreditation process follows OBM Circular A-130, and FISMA requirements. The Information Assurance Security Manager (IASM) and Information Assurance Security Officer (IASO) use a continuous monitoring model to ensure C&A compliance. A Security Development Life Cycle will be integrated with the Systems Development Life Cycle Management system and applications. A security vulnerability assessment is part of the initial requirements for certification and accreditation of the General Fund Enterprise Business System (GFEBs). While different facets of the system can be reviewed on a continuous basis, a formal security review is required every three years (or sooner for high-risk systems with rapidly changing technology or as significant changes occur). Changes to system design, architecture, and associated security controls will be approved through a System Change Request and Configuration Control Board process prior to implementation.

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.

DUE TO THE SCOPE OF GFEBs, PII IS SHARED WITH ALL ARMY COMPONENTS.

Other DoD Components.

Specify.

Defense Financial and Accounting Services, U.S. Air Force, Air National Guard, Military academy cadets and Army Reserve.

Other Federal Agencies.

Specify.

Federal Reserve banks.

State and Local Agencies.

Specify.

Department of Treasury (DOT).

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

Specify.

Accenture and EDS contractors who have access will ensure contracts specify the sensitive nature of the data and require a non-disclosure statement from each individual with access to the GFEBs system and data. Contractors will operate and manage the GFEBs system. The GFEBs contract stipulates that all GFEBs personnel (i.e., all staff with system or information access), shall have a completed background investigation prior to having access to the system, and are required to acknowledge by signature, their agreement to adhere to Army security policies and procedures prior to working on the contract. The contract includes specific security requirements required by law (FISMA, OMB, and DoD and Army).

Each contractor performing on this contract will submit its Sarbanes-Oxley, Section 404 compliance procedures, if applicable, to the Army DAA to validate the mechanisms in place at the contractor to protect the information contained in the systems. SOXA Section 404 is titled "Management Assessment of Internal Controls." It requires companies subject to the reporting requirements of the Securities Exchange Act of 1934 to include in their Form 10-K filing a report from management on its assessment of the design and operating effectiveness of the company's internal controls over financial reporting.

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.

Individuals can refuse to the collection of PII by not submitting information.

(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.

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

Once the individual consented to the collection of PII they have given implicit consent to the specific uses of their PII by providing an approved identification at an access control point.

[Empty rectangular box]

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

- Privacy Act Statement**
- Privacy Advisory**
- Other**
- None**

Describe each applicable format.

The formal collection method is written e-mail request using Digital Signature and encryption. The format of the PAS would be WEB, Paper or verbal.

In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a (b) (3).

When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.