Government Financial Information System (GFIS)

Privacy Impact Assessment

1. IT System or Electronic Information Collection Identification

a. Who is completing the initial screening assessment?

Designated Security Officer, OCFO/CFS/FSB.

b. Who is the IT system or electronic information collection owner?

Deputy Associate Director for Center of Financial Services and Deputy Chief Financial Officer, OCFO/CFS.

c. What is the IT system or electronic information collection name?

Government Financial Information System (GFIS).

d. Does the activity represent a new or significantly modified IT system or information collection?

No.

e. Is this an IT system or project or an electronic information collection?

IT System of Project.

f. What is the Unique Project Identifier (UPI)?

027-00-01-01-01-1010-00-402-124.

g. Will this IT system or electronic information collection use web technology?

Yes.

h. What is the purpose of the IT system or electronic information collection and why is the information being collected?

GFIS is used for financial management and runs on American Management System's (AMS/CGI) Momentum. GFIS provides financial planning capabilities and a means for OPM to record financial transactions. This includes documenting financial planning and purchasing events, accounts receivable and payable, disbursement, and budgeting activities.

i. What is the IT system or electronic information collection status?

Operational.

j. Is the IT system or electronic information collection operated by OPM staff, contractor staff, or a combination of OPM and contractor staff?

Combination of OPM staff and contractor staff.
CGI/Federal.

k. Where is the IT system or electronic information collection physically located?

Washington, D.C.

2. Initial Screening Assessment

a. Is an OMB mandated PIA required for this IT system or electronic information collection?

Yes.

b. Does the system or electronic information collection contain or collect any Personally Identifiable Information (PII)?

Yes.

c. Is this an IT system that collects PII on members of the public?

No.

d. Is this an electronic information collection that collects PII on members of the public?

Yes.

e. Is this an electronic information collection that collects PII on Federal employees?

No.

3. The PIA

3.1. Nature and Source of Information to Be Collected

a. What is the nature of the information to be collected?

GFIS is used for financial management and runs on American Management System's (AMS/CGI) Momentum. GFIS provides

financial planning capabilities and a means for OPM to record financial transactions. This includes documenting financial planning and purchasing events, accounts receivable and payable, disbursement, and budgeting activities.

b. What is the source of the information?

Other sources such as databases, web sites, etc.

3.2. Reason for Collection of Information

a. Why is the information being collected?

GFIS accounts payables and accounts receivables – allows OPM to provide financial planning capabilities and a means to record financial transactions.

b. Is there legal authority for collecting the information?

Yes.
Federal regulation laws and acts. Federal Managers' Financial Integrity Act (FMFIA) and Circular A-130.

3.3. Intended Use of the Collected Information

a. What is the intended use of the information?

GFIS use vendor information for purchasing events, accounts receivable, accounts payable, disbursement, and budgeting activities for OPM.

b. For major IT investments as defined in OMB Circular A-11, a high-level data flow diagram must be prepared?

Yes.

3.4. Purpose and Identification of Information to Be Shared

a. Does the system share Personally Identifiable Information (PII) in any form?

Yes.
Within OPM.
Production users of GFIS.

b. Who will have access to the PII on the system?

Users, Administrators, Developers, and Contractors.

c. Is information part of a computer matching program?

No.

3.5. Opportunities Individuals Have to Decline to Provide Information or to Consent to Particular Uses of the Information

a. Is providing information voluntary?

No.

b. Are individuals informed about required or authorized uses of the information?

Yes.
Other: Rules of Behavior.

c. Will other uses be made of the information than those required or authorized?

No.

3.6. Security of Information

a. Has the system been authorized to process information?

Yes.

b. Is an annual review of the IT system or electronic information collection conducted as required by the Federal Information Security Management Act (FISMA)?

Yes.

c. Are security controls annually tested as required by FISMA?

Yes.

d. Are contingency plans tested annually as required by FISMA?

Yes.

e. Have personnel using the system been trained and made aware of their responsibilities for protecting the PII being collected and maintained?

Yes.

f. Are rules of behavior in place for individuals who have access to the PII on the system?

Yes.
General users and System/database, administrators, developers, etc.

3.7. System of Records as Required by the Privacy Act, 5 U.S.C. 552a

a. Are records on the system routinely retrieved by a personal identifier?

Yes.
Privacy Act applies.

b. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes.
OPM Internal - 5.

c. Does the SORN address all of the required categories of information about the system?

Yes.
System name; System location; Purpose; Disclosure to consumer reporting agencies; Contesting record procedure; Notification procedure; System exempted from certain provisions of the Act; System classification; Authority of maintenance; Routine uses of records maintained; System Manager and contact information; Record access procedure; Record source categories; Policies and practices for storing, retrieving, accessing, retaining, and disposing of records.

d. Has any of the information in the SORN changed since the information was published?

Yes.

e. Are processes in place for periodic review of Personally Identifiable Information contained in the system to ensure that it is timely, accurate, and relevant?

Yes.

Review policy and the processes for retention and destruction of records complies with OPMs Records Management policy schedule 3.BUF.01.

4. Certification

A PIA is required and the OPM Chief Privacy Officer and Chief Information Officer signed the PIA approval on August 2, 2007.