Intekras/GP/SABA (IGS) Baseline Learning Management System

Privacy Impact Assessment

1. IT System of Electronic Collection Identification

a. Who is completing the initial screening assessment?

Security Engineer,
General Physics (GP).

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

Program Director,
OPM/GoLearn.

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

Intekras/GP/SABA (IGS) Baseline Learning Management System.

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 or Project.

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

N/A.

g. Will this 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?

This system is used to deliver online training for Federal clients, in support of the OMB e-training initiative.

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?

Contractor Staff.

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

Virginia.

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?

Yes.

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?

Yes.

3. The PIA

3.1. Nature and Source of Information to Be Collected

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

Individual learner data elements collected through GoLearn program are Unique Student Identifier, Social Security number, date of birth, salary, gender, race, last update of student record and last update of user ID. Only a small number of GoLearn data elements are such that the unauthorized disclosure may constitute an invasion of personal privacy with potential for adverse impact on the individual.

b. What is the source of the information?

Directly from the person to whom the information pertains;
From other people;
Other sources such as databases, websites, etc.

3.2. Reason for Collection of Information

a. Why is the information being collected?

The purpose of information collection within the GoLearn system is to provide online training courses and curriculum to Federal agencies, and for OPM to record employee training activities for Federal Government agencies as mandated by the e-Training Initiative.

b. Is there legal authority for collecting the information?

Yes.
E-Government Act of 2002.

3.3. Intended Use of the Collected Information

a. What is the intended use of this information?

Information will be used for individual learning plans, training, and development. OPM will record employee training for reporting to OMB, as required.

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.
With other Federal agencies.
Data owner (Federal agency) and OMB.

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

Users, Administrators, 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.

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, 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.

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

Yes.
US OPM GOVT-1.

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

No.

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

No.

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.
GP has a Media Protection policy in place that prescribes the procedures for retaining, reusing, or destroying records or files. In addition, GP has procedures in place to review account activity and remove inactive accounts or data after 90 days of non-use.

4. Certification

A PIA is required and the OPM Chief Privacy Officer signed the PIA on September 22, 2006.