GSA Online University (OLU) and External Learning Management System (ELMS)

Privacy Impact Assessment (PIA)

June 14, 2021

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Richard Banach - ISTF

Name of Program Manager/System Owner:

- Monica Shackelford - ICS

Signature Page

Signed:

DocuSigned by:
Richard Banach
21B998D30FCE4B6...

Information System Security Manager (ISSM)

DocuSigned by:
Monica Shackelford
0C9D8301687C4C8...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version #
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
5/11/2021	Updated IDP & SF182 entries (Per Privacy Analyst Request)	3.1
6/14/2021	Approved	3.2

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about *[system, application, or project]*. To accomplish its mission *[GSA office]* must, in the course of *[program name]*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

GSA Online University (OLU) and External Learning Management System (ELMS) – FISMA System: GSA Online University (GSAOLU) - IC-GSAOLU

B. System, application, or project includes information about:

OLU contains information about GSA Employees and Contractors only.
ELMS contains information about Federal Employees and Contractors outside GSA (i.e. those who do not have a GSA network account).

C. For the categories listed above, how many records are there for each?

- OLU – 1.2 million training course records about unique federal employees and contractors as of 2020
- ELMS – 2,000 training course records about federal employees and contractors as of 2020

D. System, application, or project includes these data elements:

OLU and ELMS contain Individual Name, Contact Information, and User Information

Overview

GSA On-Line University (OLU) learning management system serves all GSA employees and contractors. The OLU is a platform for users to have access to over 2,000 online training courses (including mandatory training and custom courses), and over 10,000 reference books. OLU is used to track online training along with the Individual Development Plan (IDP), administer the SF-182 (Authorization, Agreement, and Certification of Training), manage the registration process for instructor led training, and provides the information needed for annual Enterprise Human Resources Integration (EHRI) reporting to the Office of Personnel Management.

The specific data elements collected in the system are: Employee Number data field (numeric numbers, fed from GSA's HR Links data feed to OLU), together with other data fields (e.g., Name, Email address, Work Address, GS Level, Start Date, End Date, Region, Org Code, Job Series, and other job-related information). Courses taken and status information (who assigned the course, course start and stop times, the number of times a course has been started, and the number of failed attempts) are also collected.

PII collected:

- User Principal Name (PIV ID) for internal user identification
- Name for display and reporting purposes
- GSA Email address for SecureAuth SSO login

External Learning Management System (ELMS) serves Federal Employees and Contractors. The ELMS is a platform to provide GSA related training e.g. Fleet management, Contract processes, etc. to Federal employees and Contractors. ELMS is used to deliver and track online courses on a completed/Incomplete basis.

PII collected:

- Name for display and reporting purposes
- Email address for system login

OLU and ELMS are covered under SORNS:

- GSA/Agency-1, Employee Related Files, 61-FR-60103 - November 26, 1996
- OPM-GOVT-1, General Personnel Records, 77-FR-73694 - December 11, 2012

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information.

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

SORNs GSA/Agency-1 and OPM-GOVT -1 covering GSAs personnel and training records.

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No ICR has been submitted.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

1. Title: GRS 02.6/010 Non-Mission Employee Training Program Records.

Description: Non-mission employee training program records. Records about planning, assessing, managing, and evaluating an agency's training program: plans, reports, and program evaluations, organizational and occupational needs assessments, employee skills assessments, employee training statistics, notices about training opportunities, schedules, or courses, mandatory training tracking and reporting files, logistics and coordination documents, Authorization, Agreement, and Certification of Training

(SF-182) and similar records, registration forms, employee attendance records, syllabi, presentations, instructor guides, handbooks, and lesson plans, reference and working files on course content, other course materials, such as presentations and videos, student, class, or instructor evaluations. NOTE: Financial records related to purchase of training or travel for training are scheduled under GRS 1.1, item 010.

Exclusion: This item does not cover ethics-related training. Ethics training is scheduled by GRS 2.6, item 020.

Retention Instructions: Temporary. Destroy when 3 years old or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.

Legal Authority: DAA-GRS-2016-0014-0001 (GRS 02.6/010)

2. Title: GRS 02.6/020 Ethics Training Records.

Description: Records include but are not limited to: administration of new employee ethics orientations, annual, and other types of ethics training, agency annual written plans, notices about training requirements and course offerings.

Retention Instructions: Temporary. Destroy when 6 years old or when superseded whichever is later, but longer retention is authorized if required for business use.

Legal Authority: DAA-GRS-2016-0014-0002 (GRS 02.6/020)

In addition, the following systems information resides in the OLU/ELMS system that is used to add to the actual records in the form of directories, or other profile information of the employee or contractor. That information will be updated, managed, reported, and serve as content for system upgrades or conversions. The following record items cover use of that PII:

3. Title: GRS 02.6/030 Individual Employee Training Records.

Description: Records documenting training required by all or most Federal agencies, such as information system security and anti-harassment training, and training to develop job skills. Records may include: completion certificates or verification documents for mandatory training required of all Federal employees or specific groups

of employees (e.g., supervisors, contractors), Individual Development Plans (IDPs), mentoring or coaching agreements.

Exclusion: Academic transcripts, professional licenses, civil service exams, or documentation of mission-related training are not covered by this item."

Retention Instructions: Temporary. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use.

Legal Authority: DAA-GRS-2016-0014-0003 (GRS 02.6/030)

4. Title: GRS 04.2/130 Personally Identifiable Information Extracts.

Description: System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information.

Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet “Log and Verify.”

Retention Instructions: Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.

Legal Authority: DAA-GRS-2013-0007-0012 (GRS 04.2/130)

5. Title: GRS 04.2/140 Personally Identifiable Information Extract Logs.

Description: Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date.

Retention Instructions: Temporary. Destroy when business use ceases. Legal Authority: DAA-GRS-2013-0007-0013 (GRS 04.2/140)

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

A Privacy Banner is provided prior to the collection or sharing of personal information. Notice is also provided through SORNs GSA/Agency-1 and OPM-GOVT-1 – General Personnel Records, as well as this PIA, posted on www.gsa.gov/pia.

SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

- OLU – User Principal Name is used for internal record identification, Name for display and reporting purposes, Email address for SecureAuth SSO login.
- ELMS – Name for display and reporting purposes, Email address for system login.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

OLU and ELMS do not aggregate or derive new data.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

OLU and ELMS have implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk

assessment, system and services acquisition, system and communications protection, along with system and information integrity.

3.4 Will the system monitor the public, GSA employees, or contractors?

OLU and ELMS do not monitor GSA employees and contractors. OLU and ELMS are used for training purposes only.

3.5 What kinds of report(s) can be produced on individuals?

OLU and ELMS – Reporting on courses taken by the individual

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

OLU and ELMS do not de-identify data when reporting.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

OLU and ELMS limit information to only what is required to carry out training courses.

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

OLU – Provides information for transmission of GSA employees' training records to OPM's Enterprise Human Resources Integration (EHRI) for the Federal Government's human capital management. This disclosure is covered by SORNs OPM-GOVT-1 and GSA Agency-1.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

OLU and ELMS information collected comes from the individual's participation in the training courses.

OLU has a data feed from HR Links and GCIMS to populate employee information for logging into the system and identification for course reporting.

ELMS has a data feed from the User Registration System based upon input from individuals requesting training courses.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

Within GSA, OLU interacts with HR Links and GCIMS. ELMS interacts with the User Registration System. Please see response to 4.3 (above) for details.

Outside of GSA, OLU interfaces with SkillPort to access courses for training. SkillPort provides two types of training:

1. A training course can be requested from the SkillPort library and the course is loaded into the OLU for execution by the individual.

2. A SkillPort training course can be requested by an individual and the OLU will log the individual through SSO into SkillPort to take the course.

A contract is in place for SkillPort to provide the courses to GSA and SkillPort is FedRAMP certified.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

The PII information is uploaded daily from the system of record (HR Links and GCIMS).

Note: Daily extract from HR Links which contains the employee name and their GSA email address The GCIMS extract contains the same information for contract personnel.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

OLU and ELMS have individual and administrative role access to the data in the system. The access authorization is covered under the NIST SP 800-53 security and privacy controls defined in the System Security Plan.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes, the SSP was included in the OLU authority to operate (ATO) issued on October 4, 2017. ELMS has been documented in the OLU SSP.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

OLU and ELMS have implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, along with system and information integrity.

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

The system owner and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer, along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

The opportunities are defined under SORNs GSA/Agency-1 and OPM-GOVT-1.

7.2 What procedures allow individuals to access their information?

OLU and ELMS have a basic account created for all individuals through which they can view and update their training course information.

7.3 Can individuals amend information about themselves? If so, how?

Yes, individual information can be amended via procedures defined for the GSA Human Resources system which is uploaded on a periodic basis to the OLU and ELMS.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

Security and privacy training is given through the OLU as part of the on-boarding process and annual refresher training to all GSA employees and contractors.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

No training is provided on this specific system that requires a PIA. The security and privacy training employees receive annually covers the overall process.

---

[1]OMB Memorandum *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” The memorandum notes that “because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.”

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.