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

Privacy Impact Assessment

October 9, 2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

richard.speidel@gsa.gov

Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses 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 demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

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. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:
https://www.gsa.gov/portal/getMediaData?mediaId=167954

If you have any questions, send them to gsa.privacyact@gsa.gov.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Revised to include questions about third party services on websites and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding "Information Collection Requests"	2.1

Table of contents

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?

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)?

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

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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 for the information system(s) supporting the project?

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

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline 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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about GSA Online University (OLU) and External Learning Management system (ELMS). GSA may, in the course of using the GSA Online University (OLU) and External Learning Management system (ELMS), 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

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

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).

System, application or project includes

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, manage the registration process for instructor led training, and provides the information needed for annual 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, 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 Principle Name (PIV ID) for internal user identification.
- Name for display and reporting purposes.
- 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, 61-FR-60103 - November 26, 1996
- OPM-GOVT-1, 77-FR-73694 - December 11, 2012

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

OLU – User Principle Name (PIV ID) for internal user identification, Name for display and reporting purposes, and Email address for SecureAuth SSO login.

ELMS – Name for display and reporting purposes, Email address for system login.

1.2 What legal authority and/or agreements allow GSA to collect 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.

1.3 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 being collected?

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

1.4. Has any 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.

1.5. 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.

Records contained in the OLU and ELMS systems will be retained consistent with section 2.2 of NARA General Records Schedule, “Employee Management Records”. Disposition Authority Number: DAA-GRS-2016-0014-0001 - 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.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

The records in OLU are vital as they determine who gets network access; they play a role in performance evaluation; may inform the DHS CDM program and GSA/OMB/OPM initiatives; and could cause harm, embarrassment or inconvenience for individuals. The records stored in the system are also potentially sensitive as OLU reports can also show how long it took a person to complete a course and how many times they tried. The Privacy Act requires that we have appropriate administrative, technical and physical safeguards for such information and the PIA is GSA's privacy risk management tool.

In addition, GSA Policy CIO P 1878.2A, (1c) requires "all existing GSA systems that contain information in identifiable form about the general public are subject to the full PIA requirement and must complete an initial PIA… All GSA systems that contain information in identifiable form on Federal Government employees require a full PIA." https://www.gsa.gov/cdnstatic/CIO_P_1878.2A_Conducting_Privacy_Impact_Assessments_%28PIAs%29_in_GSA_%28Signed_on_October_29__2014%29.pdf

The E-Government Act states that, "Privacy Impact Assessments ("PIAs") are required for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form." More information may be found here: https://www.justice.gov/opcl/e-government-act-2002

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

A Privacy Act Statement 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 gsa.gov/pia.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

GSA frequently communicates with its employees and contractors about the importance of completing mandatory training and the opportunities that additional training can provide. GSA mitigates potential privacy risks related to openness and transparency through its publication of SORN GSA/Agency-1 and reference to OPM-GOVT-1 – General Personnel Records.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII 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 Whose information is included in the system, application or project?

OLU – GSA Employees and Contractors

ELMS – Federal Employees and Contractors

3.2 What PII will the system, application or project include?

OLU – User Principle Name, Name, Email address and training records

ELMS – Name, Email address and training records

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

OLU – User Principle 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.

3.4 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.

3.5 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 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.

3.6 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.

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

OLU and ELMS – Reporting on courses taken by the individual

3.8 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

The unauthorized disclosure of training records could cause harm or embarrassment; therefore, GSA will only release such information in accordance with the SORN or in a de-identified/aggregated format (e.g. 98% of GSA employees and contractors successfully completed required training on their first attempt last year). GSA also deletes the information in accordance with the records schedule, decreasing the potential risks to individuals.

SECTION 4.0 LIMITS ON USES AND SHARING OF 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 limits information to only what is required to carrying 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 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, how and is a formal agreement(s) in place?

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.

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

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

OLU sharing information with the OPM EHRI is covered under SORNs GSA/Agency-1 and OPM-GOVT-1.

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 be verified for accuracy and completeness?

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

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

Each OLU and ELMS record may pose a unique privacy risk. The records stored in the system are also potentially sensitive as these records can also show how long it took a person to complete a course and how many times they tried. GSA employs appropriate administrative, technical and physical safeguards for such information and this PIA is the system owner and GSA's privacy office risk management tool.

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 for the information system(s) or application?

OLU 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, technological, and managerial perspective?

OLU and ELMS have implemented the required security and privacy controls according to NIST SP 800-53. The systems employ 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 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

OLU and ELMS - if the data were accessed by an unauthorized individual or otherwise breached there might be possible harm or embarrassment through the disclosure of training course information.

OLU and ELMS have implemented the required security and privacy controls according to NIST SP 800-53. The systems employ 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.

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 are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline 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 amended through procedures defined for the system of record which is uploaded on periodic basis to the OLU and ELMS.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Yes, there are some privacy risks for this system that relate to individual participation as GSA employees may be assigned by their supervisor to take a particular course in order to address a performance deficiency. GSA mitigates this risk through least privilege access controls to administrative data and by promoting transparency through this PIA.

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

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

OLU and ELMS are the ways that GSA provides its employees, Federal colleagues and contractors with timely and relevant privacy training. All GSA personnel are trained on how to identify and safeguard PII. In addition, each employee must complete annual privacy and security training. Many staff receive additional training focused on their specific job duties. Those who need to access, use, or share PII as part of their regular responsibilities complete additional role-based training.

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, application or project ensure that the information is used in accordance with the stated practices in this PIA?

OLU and ELMS have implemented the required security and privacy controls according to NIST SP 800-53. The systems employ 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes, there are privacy risks for OLU that relate to accountability and auditing. Consistent with NIST 800-53 rev 4, control number AR-4, GSA frequently evaluates its programs to ensure effective implementation of privacy controls.

To alleviate these risks, GSA clearly identifies personnel with the capacity to audit its OLU program and provides them with suitable role-based training. Auditors execute their duties in concert with GSA supervisors and/or GSA's Privacy Office.

[1] OMB Memorandum *Preparing for and Responding to a 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.