Privacy Impact Assessment (PIA)

Name of Project: NARA Learning Management System

Project's Unique ID: LMS

Legal Authority(ies):	OPM's authority to require agencies to collect this information is established in Title 5, Section 2951 of the U.S. Code (5 U.S.C. 2951) and Title 5, Part 9.2 of the Code of Federal Regulations (5 CFR 9.2). NARA's obligations to protect this information is provided in NARA Directive 1608, the Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, and 5 U.S.C. § 552a), a United States federal law.

Purpose of this System/Application: The Learning Management System (LMS) provides a platform to assign, launch and deliver, and track training for internal NARA employees and external customers across the federal government. The system contains user information, course content information, and system configuration information. Access to all information is restricted by system account roles behind individual username and password authentication. Privileged users including administrators will be required to enter the system using multi-factor authentication. Content packages, including SCORM packaged content, is served from the system. Course content is launched via a course configuration accessed with an authenticated account. When accessed by an authenticated user, content communicates status and score to the LMS. The system is also used to schedule training events and capture training and training expenditures.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		The system collects transaction records for each user. Additionally, employee user profiles include the following data elements: employee ID, First Name, Middle Initial, Last Name, Email, Hire Date, Gender, RNO, Manager ID, Position ID, Work Location ID, Organization Identifier.
External Users		The system collects transaction records for each user. Additionally, employee user profiles include the following data elements: First Name, Middle Initial, Last Name, Email, Sponsoring Organization, Work Address, Work Telephone
Audit trail information (including employee log-in information)		Audit records are maintained for login, changes to any item in the system, and proxy logins (administrator logs in as a user to troubleshoot issues).

Other (describe)		

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

NARA operational records		
External users		Self-registration.
Employees		NARA's payroll provider, Department of Interior, provides data via FPPS / Datamart / OBIEE. This data includes Organization, Position, Grade, Location, Manager ID, Hire Date, Gender, RNO, Email, First Name, Last Name, Middle Initial, and Employee ID.
Other Federal agencies (list agency)		Self-registration.
State and local agencies (list agency)		Self-registration.
Other third party source		Content library (such as Skillsoft Skillport) can provide a list of titles through an integration.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes. For internal employees, the data collected is necessary for the generation of SF-182 records to OPM, which is a record of employee training. For external customers, the data collected is necessary to identify the user for progress on records management certification programs.

2. Is there another source for the data? Explain how that source is or is not used?
No other systems currently collect this data or serves this business purpose.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
Transaction records for certification programs, development programs, and compliance / required training will be generated for each user in the system that progresses in a learning object. For internal employees, SF-182 records will be filed with OPM using Enterprise Human Resource Integration system..

2. Will the new data be placed in the individual's record?

Yes, the LMS will be the system of record for documenting internal and external employees completion of training. The SF-182 requirement provides data to OPM. However, these records are not made available in the employees eOPF.

3. Can the system make determinations about employees/the public that would not be possible without the new data?

No, the system doesn't make determinations about employees or external customers except for tracking of completion and registrations for training events.

4. How will the new data be verified for relevance and accuracy?

Internal and external employees will be able to view their training record in LMS and confirm it is accurate. In the event an employee believes the system has not correctly recorded their training, they will be able to follow up with the LMS system administrators and owners to address questions or correct their records.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Data consolidation from the old system is being undertaken by internal staff within the NARA protected environment. Datafeeds shared with the vendor will be protected with FIPS 140-2 compliant PGP encryption.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Yes. Data consolidation from the old system is undertaken by internal staff within the NARA protected environment.

7. Generally, how will the data be retrieved by the user?

Each non-privileged user will have access to a limited set of their own data. Access to profile information can be suppressed by configuration. Supervisors can also view profile data with the same profile view suppression by configuration.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.
SSN is only used for SF-182 data and is not visible to users. SF-182s are only generated for NARA employees, not for external federal agency customers. Transcript records will be tied to an individual profile by an internal identifier. For NARA employees, this will be their NARA employee ID. For contractors, volunteers, and foundation employees, this will be an internal identifier unique to the LMS. OPM requires agencies include the SSN of the SF 182.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
Completion reports and test item analysis. These reports and dashboards will be accessible by report users, program coordinators, content managers, and supervisors. Completion reports are used to track progress in development programs and compliance / required training.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
Yes. External accounts for non-privileged users will not use Single Sign-on / Multifactor Authentication. External accounts will be generated through self-registration. Internal NARA employees, including privileged users (supervisors, report accounts, instructors, coordinators, administrators) will need to access the system using SSO/MFA.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.
Yes. To track registrations for training events and learning objects and to report completion within the security scope of the reporting user. For example, supervisors can only see transaction history for employees within their span of control. Supervisors cannot see transaction information for another office outside of their span of control.

12. What kinds of information are collected as a function of the monitoring of individuals?
Transaction records for training events and learning objects. Development goals and planning activities for internal employees.

13. What controls will be used to prevent unauthorized monitoring?
Managers, supervisors and system administrators are assigned additional roles and have visibility into how end-users in their unit are completing training. In addition, all actions in the system are captured and logged so that they may be reviewed for unauthorized actions.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
Yes. However, persistent cookies are only used to help maintain application state.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?
Supervisors, managers, and administrators. Users will have access to their own information.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?
Application controls, documented in the System Security Plan and system documentation, are implemented through security roles. Access by privileged users can be terminated within the system by an administrator or by terminating access through single sign-on.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
Users will be restricted by role. Most users will only have access to their own data. Supervisors will have access to their own data and those of direct and indirect reports. Program coordinators will have access to user data relevant to their program. Administrators can be constrained by capability assignment or organizational assignment (can only administer Research Services, for example).

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?
Administration users will be provided a user security agreement that includes a rules of behavior section similar to FPPS, WTTS, and DATAMART. These signed records will be maintained by HSB.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? **If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**
Yes. Privacy Act clauses were inserted in the contract.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.
FPPS / Datamart / OBIEE provides user profile information for NARA federal employees.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?
FPPS / Datamart provided by Department of Interior, IBC.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
Each privileged user.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.
Other agency users can see their own data. OPM SF-182 data delivered through a secure routine. OPM data standards for human resources. http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?
To access the system, users must provide consent.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
The system is not used to generate negative determinations.

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).
The system security plan will address the security of the data. Each individual user will be able to validate the accuracy, timeliness, and completeness of the information about them, and, in the case of NARA employees, supervisors will be able to validate that information as well for the employees they supervise.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
While the system can be accessed from any location, the management of the data is centralized.

3. What are the retention periods of data in this system?
Compliance / required training records, except one-time requirements, will be retained 6 years past cut-off. All other transcript records will be maintained for 20 years or a Federal Employee's retirement, whichever is longer.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

Records that reach the end of retention will be marked and will be excluded from reports. Like most LMS systems, this system does not permanently delete data as irretrievable deletion is a risk to data integrity. However, records can be suppressed from reports.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

Single sign-on using NARAnet logins was not previously used. This will enhance data security.

6. How does the use of this technology affect public/employee privacy?

No differently than the previous system. Privacy is maintained as described in previous sections of this document.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

Yes. The system is FedRAMP authorized, as documented at fedramp.gov.
Additionally, the system will not go live without a NARA ATO following a security evaluation.

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

A risk assessment is in process as part of the security evaluation and any identified risks will be managed as part of a plan of action and milestone for the system.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

Access reports and audit reports provide a method for evaluating access, modification, and reporting.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Steven.flowers@nara.gov.

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.
NARA 5

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
Yes. SORN will be modified to document changes to platform.

Conclusions and Analysis

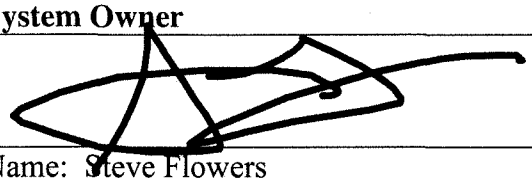
1. Did any pertinent issues arise during the drafting of this Assessment?
No.

2. If so, what changes were made to the system/application to compensate?
N/A

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Owner	
 (Signature)	11/18/2016 (Date)
Name: Steve Flowers	
Title: Chief, Organizational Development Branch, Office of Human Capital	
Contact information: steve.flowers@nara.gov	
Senior Agency Official for Privacy (or designee)	
GARY STERN Digitally signed by GARY STERN DN: c=US, o=U.S. Government, ou=National Archives and Records Administration, cn=GARY STERN, 0.9.2342.19200300.100.1.1=88001000069125 Date: 2016.11.18 11:39:07 -05'00' (Signature)	(Date)
Name: Gary M. Stern	
Title: General Counsel and SAOP	
Contact information: garym.stern@nara.gov	
Chief Information Officer (or designee)	
Swarnali Halder (Signature)	11/22/2016 (Date)
Name: Swarnali Halder	
Title: CIO	
Contact information: swarnali.halder@nara.gov	