ADAMS ML18086B178

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Learning Management System (LMS)

Date: March 23, 2018

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Learning Management System (LMS) is a Software-as-a-Service (SaaS) cloud service that is used to manage the development, delivery, and tracking of training under the direction of the Office of the Chief Human Capital Officer (OCHCO).

The purpose of the system is to provide employees, their supervisors, and human resources and training departments with more efficient means to manage the learning aspects of human resource management functions by leveraging the commercial-off-the-shelf (COTS) SAP SuccessFactors Human Capital Management (HCM) Suite. The learning portion of the HCM suite is referred to as the Learning Management System (LMS).

LMS is a cloud service with a Provisional Authority to Operate (P-ATO) granted by the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) in November 2017. The full name of the cloud service as specified in the FedRAMP authorization package is "SAP NS2 Cloud – SuccessFactors HCM Suite for Government."

LMS is also referred to as the Success Factors Baseline Learning Management System (SB_LMS).

The cloud service provider (CSP) responsible for delivery of this SaaS cloud service is SAP National Security Services, Inc. (SAP NS2).

2. What agency function does it support?

LMS provides the agency with a robust process for handling training development, delivery, administration, and monitoring functions. The administration/monitoring functions include a compliance tracking capability that is especially important for the regional offices and the new employee development programs.

LMS assists NRC to comply with e-Learning standards, while providing a broad range of capabilities to enable program management and tracking relevant to training efforts, curriculum development, and delivery of a variety of training courseware content.

One of the goals for the agency and OCHCO is to sustain a high-performing, diverse workforce. Training is a vital part of ensuring that the agency staff has the knowledge, skills, and abilities to successfully carry out the agency's mission. The agency advances continuous learning as a strategic business investment. The well-developed LMS supports and advances federal and agency priorities as well as enhances human capital initiatives by supporting/leveraging existing training resources and providing a focal point for their access.

Furthermore, the LMS cloud platform provides the agency significant flexibility through allowing the agency to focus solely on the management of learning while the FedRAMP CSP maintains the lion's share of responsibility for the operations and management (O&M) of the service. Additionally, the cloud platform has the ability to scale and support increased demand by the agency as needed over time.

3. Describe any modules or subsystems, where relevant, and their functions.

While other modules exist, the agency is only using the LMS module of the HCM Suite.

4. What legal authority authorizes the purchase or development of this system?

Federal agencies are required to collect detailed information on training programs and needs, and to electronically report the data to the Office of Personnel Management (OPM) per 5 CFR 410 per; RIN 3206-AK46; 71 Fed. Reg. 28,545.

5. What is the purpose of the system and the data to be collected?

In general, OCHCO and other NRC staff use the data input to, and collected by, the system to:

- *manage and track training efforts, including training and curriculum development, delivery, administration, and monitoring functions,*
- *review the status of open and completed training,*
- *analyze trends based on training activity, and*
- *prepare and submit standard reports, NRC-developed reports, and-hoc query results as needed*

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Andrey Korsak	*OCHCO/ADHRTD/LOPIB*	*301-287-0574*
Business Project Manager	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz	*OCHCO/HCAB*	*301-287-0805*
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Brendan Cain	*OCHCO/HCAB*	*301-287-0552*
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Miriam Cohen	*OCHCO*	*301-287-0747*

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System __X__ Modify Existing System ____ Other (Explain)

b. If modifying an existing system, has a PIA been prepared before?

Yes

.

(1) If yes, provide the date approved and ADAMS accession number.

ML061180268, May 25, 2006

(2) If yes, provide a summary of modifications to the existing system.

The NRC will migrate data, as needed, from the existing LMS application to the SaaS LMS cloud service. NRC will cease use of

the existing LMS application in the future at a point following implementation of the new service.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes.

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Information may be obtained for the following groups of individuals:

- *NRC employees*
- *NRC contractors*
- *Agreement State employees*
- *Other government agency employees (e.g., Army, Navy, Air Force, Federal Bureau of Investigations [FBI])*
- *Other nations' regulatory agencies (International Atomic Energy Association [IAEA] member countries) employees*

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

Agency training records: Name, social security number (SSN), date of birth, office/organization, position, grade, e-mail address, training dates, course and session information, cost, approvals, training facility

Please note that names will be maintained for NRC employees and NRC contractors, however, social security numbers (SSN) will only be maintained for NRC employees.

c. Is information being collected from the subject individual?

Yes. To the greatest extent possible, efforts are taken to collect information about an individual directly from the individual.

(1) If yes, what information is being collected?

Information from NRC employees: Name, social security number, date of birth, office/organization, position, grade, , e-mail address, training dates, course and session info, cost, approvals, training facility.

Information from NRC contractors: Name, office/organization, e-mail address, training dates, course and session info, cost, approvals, training facility.

Information from Agreement State employees, other government agency employees (e.g., Army, Navy, Air Force, FBI), and other nations regulatory agencies (IAEA member countries) employees: Name, affiliation, e-mail address, and course/session information.

Data will not be collected from Federal contractors directly. Information that is collected from Federal contractors is obtained and input into LMS by OCHCO and NRC staff across all offices with this job function as part of their role in the system.

d. Will the information be collected from 10 or more individuals who are not Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?

Yes. OMB approval has been obtained for information collected by LMS public respondents, such as Agreement States, is used to identify participants in NRC training courses.

(a) If yes, indicate the OMB approval number:

This collection of information is covered under OMB Clearance Number 3150-0029. *Around October 1 each year, the Office of Nuclear Material Safety and Safeguards (NMSS) sends a memo to all Agreement States notifying them of upcoming NRC training courses. Agreement States wishing to participate in these courses fill out a training application and submit the application to NMSS.*

NMSS gathers information regarding course participants and enters the information into LMS. Agreement State information consists of student name and Agreement State abbreviation.

e. Is the information being collected from existing NRC files, databases, or systems?

Yes.

(1) If yes, identify the files/databases/systems and the information being collected.

Data on individuals is being collected from other NRC files and databases, including the Human Resources Management System (HRMS), the Department of the Interior (DOI)/Federal Personnel Payroll System (FPPS), and the NRC Enterprise Identity Hub (EIH).

f. Is the information being collected from external sources (any source outside of the NRC)?

No.

(1) If yes, identify the source and what type of information is being collected?

Not applicable (N/A)

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Per the FedRAMP PIA, the Government Agency is responsible for validating, verifying, and ensuring the integrity of any information not collected directly from the subject individual that is maintained in the system. Additionally, the FedRAMP PIA specifies that the Government Agency (in this case, NRC) utilizing this cloud SaaS offering is responsible for determining that the PII data is accurate and current in the system because the Government Agency is the originating source and maintainer of the PII data.

h. How will the information be collected (e.g. form, data transfer)?

Information will be collected through forms and data transfer.

Data on individuals is being collected in forms, such as the Agreement State application forms mentioned in 1(d)(1)(a) above, and is also being

transferred, from other NRC files and databases including the HRMS and DOI/FPPS.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

No.

(1) If yes, identify the type of information (be specific).

N/A

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

N/A

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

The data will be used to manage the development, delivery, and tracking of training under the direction of OCHCO. For instance, the data input to and collected by the system will be used by OCHCO to manage and track training efforts, review the status of open and completed trainings, potentially to analyze trends based on training activity, to prepare and deploy a variety of trainings, and to run ad-hoc queries as needed.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes. Without the data maintained in LMS, OCHCO would not be able to fulfill its mission to collect detailed information on training programs and electronically reporting the data to OPM through the Enterprise Human Resources Integration (EHRI) program, per 5 CFR 410 per; RIN 3206-AK46; 71 Fed. Reg. 28,545.

3. Who will ensure the proper use of the data in this system?

The Third Party System (TPS) Information System Security Officer (ISSO), Natalya Bobryakova, and the OCHCO Technical Project Manager, Brendan Cain, will both ensure proper use of the data in LMS.

4. Are the data elements described in detail and documented?

Yes.

a. If yes, what is the name of the document that contains this information and where is it located?

The data elements are currently documented by the CSP and are located at the CSP's site.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Yes, queries could be transformed into reports that could be aggregated.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

Queries are transformed into reports that could be aggregated or stored. As far as how it is stored, the CSP provides the functionality that enables OCHCO to dynamically provision and de-provision compute, memory, and storage resources, and to be able to flexibly scale services (up or down) to meet NRC needs. Data storage and retention for any aggregation logic developed to query any LMS or feeder system data are based on the requirements specified for each report generated by LMS.

b. How will data be validated for relevance and accuracy?

Data is validated through system edits implemented by the CSP, and reviewed by authorized, authenticated users, and can only be modified to address discrepancies by those staff with that responsibility and access. For any information that may be self-reported, OCHCO does not question the accuracy of the data unless there is a reason to do so.

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

Data that are consolidated can only be accessed by authorized, authenticated users, and can only be modified by those staff with that

responsibility and access. Role-based access control (RBAC) is implemented in LMS to control access to the system and to prevent unauthorized use. Roles are defined for each authorized user, which prevents authorized users from accessing other parts of the system. Authorized users of LMS are strongly authenticated to the system.

The administrators follow the annual Privacy Act guidance for storage and disposition of data and reports. Regular audits of data and records are also performed.

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

Training records data can be retrieved by a personal identifier, such as Employee ID or LAN ID, or by the individual's name. Data can only be retrieved by authorized, authenticated user with a data description.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

a. If yes, explain.

N/A

(1) What controls will be used to prevent unauthorized monitoring?

N/A

8. List the report(s) that will be produced from this system.

Standard and NRC-developed reports will be produced from this system and include Training Reports, External Training Reports, User Reports, and System Reports.

***a.* What are the reports used for?**

Training Reports provide data on training items, registrations, training completions, curricula status, scheduled offerings, exams, and training evaluations.

External Training Reports provide data on external training requests, approvals, and verification status.

User Reports provide data on users, supervisors and their profiles.

System Reports provide data on system transactions, audit logs, and reports to generate metrics.

Furthermore, administrators run reports based on their reporting requirements, job functions, and business needs. The below list provides the common data elements included in these reports.

- *User name*
- *User email*
- *User office*
- *User type and status*
- *User training completions*
- *User registrations*
- *User external requests*
- *User approval status*
- *User curriculum status*
- *User assignment status*
- *Evaluation data*
- *Course list*
- *Scheduled offering list*

b. Who has access to these reports?

The access to the reports is managed through implementation of role-based permissions. Each group of administrators have access to reports based on their job requirements and business needs.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

The OCHCO administrators and following user groups across all NRC offices have non-privileged access to data that pertains to them individually as part of their role in the system:

- *Employees*
- *Supervisors*

(1) For what purpose?

Role-based access control (RBAC) is used in LMS to limit access to the system and to prevent unauthorized use. Authorized NRC office staff and NRC contractors with the appropriate role can access LMS such as OCHCO administrators, and the NRC office employees, supervisors, and potentially NRC contractors that require access to perform job functions

such as program management and tracking relevant to training efforts, curriculum development, and delivery and development through a variety of training courseware content.

Roles are defined for each authorized user, which prevents authorized users from accessing other parts of the system. Users are strongly authenticated to the system. Authorized NRC office staff and NRC contractors with the appropriate role are the only individuals that are authorized users of LMS.

LMS user roles are divided into two groups: NRC users and Non-NRC users. NRC user profiles are assigned to NRC employees and NRC contractors that have been authorized to access their training data including their account profile, assigned training(s), training catalog, registration process, and external training. Non-NRC user profiles are assigned to individuals such as Agreement State employees, International students, and other Federal students, and do not provide access to the LMS system. Non-NRC users are assigned accounts that are only used as placeholders for registration purposes.

The users of LMS that have been identified as Supervisors are first assigned to an NRC user profile to assign the minimum permissions, and have multiple permission sets for additional workflows to manage their direct subordinates including assign training, approve training, and run training reports.

The following table identifies the common Administrator Groups associated with NRC office staff and NRC contractors who are approved and authorized individually by the ISSO access to the appropriate group of permissions and additional permission sets as required by the needs of the business and the individual's job functions. Additionally, the administrators follow the annual Privacy Act guidance for storage and disposition of data and reports.

Administrator Group	**Purpose**
Training Coordinator	*Manages registrations, completions, and assignments.*
External Training Approver	*Manages and approves external training requests.*
Course Administrator	*Manages design and delivery of online and classroom training.*
Curriculum Administrator	*Manages curricula.*
Content Administrator	*Manages online courses, content and exams.*
Instructor	*Monitors scheduled offerings. Access to registration, evaluations, completion, and roster reports.*

Reporter	*Accesses and runs standard and NRC-developed reports that provide information about users, completions, evaluations, registrations, assignments, training status, and curricula.*
User Manager	*Creates, de-activates, and manages user accounts in the system.*
Training Support	*Answers support questions, manages registrations, assigns training, runs reports, and sends notifications.*
Power Administrator	*Manages scheduled offerings, completions, registrations, items, users, curricula, and evaluations.*
Super Administrator	*Manages the overall system. Has access to all workflows.*

(2) Will access be limited?

Yes. User access is restricted. RBAC limits access to the authorized users depending on their limits to the data individually as part of their role in the system. For instance, users of LMS may be authorized to utilize the training development, delivery, administration, and monitoring functionality of the system. In addition, they may be able to use the administration/monitoring functions, which include a compliance tracking capability that is especially important for the regional offices and the new employee development programs.

2. Will other NRC systems share data with or have access to the data in the system?

Yes.

(1) If yes, identify the system(s).

EIH

(2) How will the data be transmitted or disclosed?

A scheduled report is run on a daily basis and sent via email to the ICAMSupport.Resource@nrc.gov resource mailbox.

3. Will external agencies/organizations/public have access to the data in the system?

Yes; however, it will not be directly accessible.

(1) If yes, who?

Training completion data is transmitted in a flat file via an encrypted connection to OPM's EHRI Data Warehouse by the CSP on behalf of NRC.

(2) Will access be limited?

No external agencies/organizations/public have direct access to the data in the system.

(3) What data will be accessible and for what purpose/use?

Training records will be used by OPM to manage and track training efforts, and potentially to analyze trends based on training activity.

(4) How will the data be transmitted or disclosed?

The CSP transmits the data via secure, encrypted connections as specified by OCHCO on behalf of OPM.

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

Yes. The records and information identified in the system are Federal records that are covered under the following General Records Schedules (GRS).

GRS 2.6, Item 10, Non-mission employee training records. Disposition: 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.

GRS 2.6, Item 20, Ethics training records. Disposition: 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.

GRS 2.6, Item 30, Individual employee training records. Disposition: Temporary. Destroy when 6 years old or when superseded, whichever is later, but longer retention is authorized if required for business use.

b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records <u>cannot</u> be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

F. <u>TECHNICAL ACCESS AND SECURITY</u>

1. Describe the security controls used to limit access to the system (e.g., passwords).

The OCHCO agency administrators determine user rights and permissions for all users. All users must authenticate in order to access the LMS web application. OCHCO will to use the Information Technology Infrastructure (ITI) Identity, Credential, and Access Management (ICAM) authentication gateway (e.g. EHI) for all user authentication to LMS

Per the FedRAMP SSP, "The Government Agency is responsible for all aspects of management of Government authenticators used to log into the Federal Node HCM Suite web application to include the HSPD-12 smart card, such as the DOD CAC or PIV smart card and privilege level account implementations."

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

Access to LMS is role-based. OCHCO agency administrators are responsible for ensuring that NRC LMS users are only assigned the least role(s) and permissions necessary for them to perform their job. The LMS ISSO must approve all user roles/permissions. OCHCO relies on SAP NS2 (CSP) for the enforcement of LMS role-based access authorizations.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes.

(1) If yes, where?

The System Security Plan (SSP), which is under development, will document the criteria, procedures, controls, and responsibilities regarding access.

4. Will the system be accessed or operated at more than one location (site)?

LMS is a web application and can be accessed at all NRC sites as well as all other locations that users may be located.

a. If yes, how will consistent use be maintained at all sites?

SAP maintains the system and maintains consistent use of the system and data. As provided by the FedRAMP authorized Amazon Web Services GovCloud, the GovCloud region consists of multiple physical data centers that are all part of the same FedRAMP authorization and utilize the same controls, policies, and procedures in order to maintain consistent use of the system and the PII data. The system application software also maintains the same controls, policies, and procedures across all the GovCloud availability zones in order to maintain consistent use of the both PII and non-PII data.

Additionally, OCHCO agency administrators have the ability to obtain audit records on NRC's use of LMS.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

OCHCO agency administrators. The following user groups across all NRC offices have non-privileged access to data that pertains to them individually as part of their role in the system:

- *Employees*
- *Supervisors*

6. Will a record of their access to the system be captured?

Yes.

a. If yes, what will be collected?

OCHCO relies on SAP NS2 (CSP) to regularly audit and review event logs. Additionally, OCHCO agency administrators have the ability to obtain and review audit records on NRC's use of LMS.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes. SAP is the CSP and is responsible for the development and maintenance of LMS.

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

OCHCO relies on the CSP to be responsible for implementing front-end security, protecting the data, and ensuring that only the authorized users can access it. The CSP translates these functional requirements into the technical design and implementation.

OCHCO relies on the CSP to employ auditing measures and technical safeguards to prevent misuse of data. Additionally, OCHCO agency administrators have the ability to obtain and review audit records on NRC's use of LMS.

SAP NS2 LMS software components are configured to United States Government Configuration Baseline (USGCB), Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs), and vendor hardening guidelines.

9. Are the data secured in accordance with FISMA requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed?

LMS is part of the SAP SuccessFactors HCM Suite SaaS, which received a FedRAMP authorization on November 13, 2017.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: Learning Management System (LMS)

Submitting Office: Office of the Chief Human Capital Officer

A. PRIVACY ACT APPLICABILITY REVIEW

X Privacy Act is not applicable.

___ Privacy Act is applicable.

Comments:
Currently covered under System of Records, NRC-19, Official Personnel Training Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	5/11/2018

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

X Currently has OMB Clearance. Clearance No. **3150-0029**

Comments:

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	4/19/2018

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	5/3/18

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date May 15, 2018

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: Miriam Cohen, Chief Human Capital Officer, Office of the Chief Human Capital Officer	
Name of System: Learning Management System (LMS)	
Date ISB received PIA for review: **March 23, 2018**	Date ISB completed PIA review: **May 11, 2018**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ May 15, 2018**
Copies of this PIA will be provided to: *Tom Rich, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Services Division* *Office of the Chief Information Officer*	