

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.

Please do not enter the PIA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team.

Talent Management System (TMS)

Date: January 05, 2021

A. GENERAL SYSTEM INFORMATION

- 1. Provide a detailed description of the system:** *(Use plain language, no technical terms.)*

The Talent Management System (TMS) is a Software-as-a-Service (SaaS) cloud solution that provides the U.S. Nuclear Regulatory Commission (NRC) with an online learning platform and tools for the automation of performance management tasks and strategic workforce planning. TMS is operated by Cornerstone OnDemand, Inc. (CSOD) on their cloud platform, the Cornerstone OnDemand – Unified Talent Management Suite (CUTMS).

TMS utilizes the CUTMS Learning Management and Performance Management modules to deliver web-based, instructor-led training and automation of performance management tasks. The CUTMS Learning Management System assists the NRC in complying with e-Learning standards and provides a broad range of capabilities to enable program management and tracking relevant to training efforts, curriculum development, and delivery of a variety of training courses. The CUTMS Performance Management module assists the NRC in the development of employee performance appraisals and allows the use of competency models for skill management and strategic workforce planning.

- 2. What agency function does it support?** *(How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)*

The TMS supports the following agency functions:

- Storage of training records, course catalog, learning content management, course scheduling, and online course registration
- Management and use of competency models to support the individual development plans and close skill gaps

- Automation of performance management tasks, including development of employee performance appraisals and skill management

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

TMS is comprised of the following modules:

- Learning Management module to manage the development, delivery, and tracking of training
- Performance Management module to automate performance, skill, and competency management tasks

4. What legal authority authorizes the purchase or development of this system? (*What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.*)

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 Code of Federation Regulations (CFR) 410 per; Regulation Identification Number (RIN) 3206-AK46; 71 Fed. Reg. 28,545.

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

The Office of the Chief Human Capital Officer (OCHCO) and NRC staff use the data collected by the system to:

- Manage and track training efforts, including training and curriculum development, training delivery, administration, monitoring functions, and reporting requirements
- Review the status of open and completed training
- Analyze trends based on training activity
- Prepare and submit standard reports, NRC-developed reports, ad-hoc query results as needed
- Performance reviews and appraisals
- Competency and skills management

6. **Points of Contact:** (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.*)

Project Manager	Office/Division/Branch	Telephone
Andrey Korsak	OCHCO/ADHRTD/LTDB	301-287-0574
Business Project Manager	Office/Division/Branch	Telephone
Andrey Korsak	OCHCO/ADHRTD/LTDB	301-287-0574
Technical Project Manager	Office/Division/Branch	Telephone
Andrey Korsak	OCHCO/ADHRTD/LTDB	301-287-0574
Executive Sponsor	Office/Division/Branch	Telephone
Mary Lamary	OCHCO	301-415-3300
ISSO	Office/Division/Branch	Telephone
Natalya Bobryakova	OCIO/ITSDOD/SOB/IAT	301-287-0671
System Owner/User	Office/Division/Branch	Telephone
Mary Lamary	OCHCO	301-415-3300

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

- a. New System
 Modify Existing System
 Other

- b. **If modifying or making other updates to an existing system, has a PIA been prepared before?**

Yes.

- (1) **If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.**

A Privacy Impact Assessment was approved on June 4, 2019, ADAMS accession number ML19067A187.

- (2) **If yes, provide a summary of modifications or other changes to the existing system.**

- Updated general system information
- Updated Points of Contact table
- Updated information types maintained in the system

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

Yes.

- a. **If yes, please provide the EA/Inventory number.**

TMS is a component of the NRC's Third Party System – Talent Management (TPS-TM) subsystem. The TPS EA number is 20180002.

- b. **If no, please contact [EA Service Desk](#) to get the EA/Inventory number.**

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 (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).**

TMS maintains information about NRC employees, NRC contractors, and Agreement State employees.

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

- b. What information is being maintained in the system about an individual (be specific – e.g. Social Security Number (SSN), Place of Birth, Name, Address)?**

TMS maintains the following information about individuals:

- Name
- Office/Organization
- Training related data
- Education history
- E-mail addresses
- Course history
- Performance Reviews

- c. Is information being collected from the subject individual? (To the greatest extent possible, collect information about an individual directly from the individual.)**

Yes. To the greatest extent possible, information maintained in TMS is collected from the subject 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, and training facility.

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

Information from Agreement State Employees and External Users (I.e. other federal, international): Name, affiliation, e-mail address, work phone number, and course/session information.

Around October 1st each year, the Office of Nuclear Material Safety and Safeguards (NMSS) sends a memo to all Agreement States to notify them of upcoming NRC training courses. Agreement States that wish to participate in these courses must fill out a training application and submit the application to NMSS.

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

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

Yes.

(1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?

Yes.

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

This collection of information is covered under OMB Clearance Number 3150-0029. Around October 1st each year, NMSS sends a memo to all Agreement States to notify them of upcoming NRC training courses. Agreement States that wish to participate in these courses must fill out a training application and submit the application to NMSS. NMSS gathers information regarding course participants and enters the information into TMS. 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.

TMS collects information about individuals from Electronic Official Personnel Folder, the Human Resource Management System (HRMS), Federal Personnel Payroll System, and 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?

N/A.

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

Information collected from HRMS and an employee's personnel folder has been verified by the employee and an approving official. Employees can modify some data within their personnel folder through Employee Express. All human resource (HR) data is reviewed and verified by HR personnel.

EIH data has been verified by the Identity, Credential, and Access Management System.

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

Information about individuals is transferred from existing NRC files and databases. Information about individuals is also collected in forms, such as the Agreement State application forms.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Yes.

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

The TMS contains the NRC training catalog with descriptions of the provided courses, agency training requirements, computer-based training, live training courses, and training reviews.

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

Web-based training and curriculum information is provided by internal agency personnel with authorized access to the system. TMS also incorporates courses provided by other organizations or government agencies.

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, identify skills gaps and competency models for career development and workforce planning. 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.

In addition, TMS will report performance appraisals and training compliance in accordance with OPM mandates and will allow for the implementation, management, tracking, and reporting of performance-related tasks and items, including performance plans and appraisals.

1. 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 TMS, 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.

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

The NRC TMS administrators ensure that users are only assigned the privileges or permissions required by their job function.

3. 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?

CSOD maintains the documents that describe the data elements permitted within the system. Those documents are located on the CSOD's client community website accessible to the customers. There are at least 11 documents that describe data elements for each of the modules or functions of the system.

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

Yes, the queries could be run to create reports that aggregate data.

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?

Data is reviewed by authorized users and can only be modified to address discrepancies by staff with the necessary permissions within the system. NRC makes training completion reports available on the OCHCO website and reports performance and training data to OPM.

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

The aggregated data is reviewed and analyzed by NRC authorized users that can validate the data and address data discrepancies through system features implemented by CSOD, the Cloud Service Provider (CSP). NRC does not aggregate self-reported data within TMS.

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

Consolidated data can only be accessed by authorized NRC users who have access to the data that is necessary to perform their job responsibilities. Role-based access control (RBAC) is implemented in TMS to control access to the system and to prevent unauthorized use.

Administrators follow the annual Privacy Act (Management Directive 3.2) guidance for storage and disposition of data and reports. Regular audits of data and records are also performed.

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

Training records data can be retrieved by a personal identifier, such as Employee ID, Local Area Network Identification (LAN ID), or by the individual's name. Data can only be retrieved by authorized, authenticated user with the required access permissions.

a. **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

- Employee ID
- LAN ID
- Individual's name

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

Yes.

a. **If "Yes," provide name of SORN and location in the Federal Register.**

Official Personnel Training Records – 19.

7. **If the information system is being modified, will the SORN(s) require amendment or revision?**

N/A.

8. **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.

9. **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 Completion Reports, External Training Reports, User Reports, skills competency, and performance reports.

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

Automated reports regarding training and performance management are sent to OPM in compliance with federal reporting requirements.

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.

Performance reports will contain information regarding performance appraisals, skills gaps, and career development.

System Reports provide data on general system functionality, such as system transactions and audit logs.

b. Who has access to these reports?

The access to the reports is managed through implementation of role-based permissions. Each group of administrators has access to reports based on their job requirements and business needs. In addition, reports on completed trainings are stored on a shared drive and made available on the OCHCO website. Automated reports regarding training are also sent to OPM.

D. ACCESS TO DATA

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

OCHCO administrators, employees and supervisors across all NRC offices have non-privileged access to data that pertains to them individually as part of their role in the system.

(1) For what purpose?

Authorized NRC office staff and NRC contractors will have access to take available agency training. RBAC allows OCHCO administrators, NRC office employees, supervisors, and potentially NRC contractors to perform program management functions including:

- tracking relevant training efforts
- developing curriculums
- delivery and development of training courseware content
- management of individual competencies and skills
- performance appraisals

(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. TMS users are authorized to utilize the training development and performance information. Other privileged users will be able to use administrative functions, which include a compliance tracking capability and account administration.

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).

The EIH.

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

A scheduled report of security awareness training compliance is run daily 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.

(1) If yes, who?

Training completion data is transmitted to OPM's EHRI Data Warehouse.

(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 and performance records will be used by OPM to manage and track training efforts and individual performance and competencies.

(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 AND INFORMATION MANAGEMENT (RIM) - 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 NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA’s Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.

1) **Can you map this system to an applicable retention schedule in [NRC’s Comprehensive Records Disposition Schedule \(NUREG-0910\)](#), or NARA’s [General Records Schedules \(GRS\)](#)?**

Yes.

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).**

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

Type of Record	GRS Number	Records Title	Disposition
Training	GRS 2.6 item 010	Non-mission employee training program records	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.
Training	GRS 2.6 item 020	Ethics training records	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.
Training	GRS 2.6 item 030	Individual training records	Temporary. Destroy when 6 years old or when superseded, whichever is later, but longer retention is authorized if required for business use.

Performance	GRS 2.2 item 070	Employee performance file system records. Acceptable performance appraisals of non-senior executive service employees.	Temporary. Destroy no sooner than 4 years after date of appraisal, but longer retention is authorized if required for business use.
Performance	GRS 2.2 item 071	Employee performance file system records. Unacceptable performance appraisals of non-senior executive service employees.	Temporary. Destroy after employee completes 1 year of acceptable performance from the date of written advance notice of proposed removal or reduction-in-grade notice. This disposition instruction is mandatory; deviations are not allowed.
Performance	GRS 2.2 item 072	Employee performance file system records. Records of senior executive service employees.	Temporary. Destroy no sooner than 5 years after date of appraisal, but longer retention is authorized if required for business use.
Performance	GRS 2.2 item 073	Employee performance file system records. Performance records superseded through an administrative, judicial, or quasi-judicial procedure.	Temporary. Destroy when superseded. This disposition instruction is mandatory; deviations are not allowed.
System Reports	GRS 3.1 item 020	Information technology operations and maintenance records.	Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.
ADAMS Documents		*NUREG 0910, 2.13.7.a(4) – Training Aids	ADAMS PDFs/TIFFs are Permanent. Transfer to NARA when 10 years old.
		NUREG 0910, 2.13.7.b(4) – Training Aids from other agencies or private institutions.	ADAMS PDFs/TIFFs are Temporary. Cut off electronic files when superseded or determined to be obsolete. Destroy 1 year after cutoff.

b. If no, please contact the [RIM](#) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

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

The OCHCO Administrator is responsible for managing rights and permissions that are controlled at the customer level. The Administrator is also responsible for assigning administrative privileges within the NRC domain. Users authenticate to the system with their NRC LAN credentials. TMS relies on the Information Technology Infrastructure Identity, Credential, and Access Management authentication gateway to authenticate all users.

Any users without NRC LAN credentials, such as Agreement State employees, will require a separate username and ID.

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

Access to TMS is role-based. Agency administrators are responsible for ensuring that users are only assigned the least role(s) and permissions necessary for them to perform their job. CUTMS enforces role-based access authorizations after the accounts have been provisioned.

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

Yes.

- (1) If yes, where?**

The Talent Management (TM) System Security Plan (SSP) (ML19113A117) and the TMS operating procedures document the criteria, procedures, controls, and responsibilities regarding access.

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

No.

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

N/A.

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

Employees, contractors, and supervisors across all NRC offices have access to information that pertains to them individually. Different roles exist within the system for various levels of privileged access.

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

Yes.

a. If yes, what will be collected?

NRC relies on CSOD to regularly analyze audit records and monitor the system for inappropriate or unusual activity. NRC can request audit records containing access records and changes made by each user.

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

Yes. CSOD is the CSP responsible for the development and maintenance of the TMS.

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

- *Federal Acquisition Regulation (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?

NRC relies on the CSP to secure all data in accordance with agency wide mandates and ensure that only authorized users can access the system. The CSP implements functional requirements into the technical design and implementation of the system and undergoes annual assessments to test the current safeguards.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

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

CSOD received a Federal Risk and Authorization Management Program authorization for CUTMS SaaS on February 2, 2016.

NRC authorized TMS as a component of TPS-TM on July 17, 2019.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMSD/CSB Staff)

System Name: Talent Management System (TMS)

Submitting Office: Office of the Chief Information Officer (OCIO)

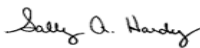
A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

This system is covered under System of Records, NRC 19, Official Personnel Training Records.

Reviewer's Name	Title
 Signed by Hardy, Sally on 01/28/21	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION


No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:


Currently the TMS does not need an OMB Clearance since it does not collect information directly but uses information on non-Federal employees provided by other sources. If changes are made to the system to directly collect information from non-Federal employees, the need for an OMB clearance will need to be revisited.

Reviewer's Name	Title
 Signed by Cullison, David on 01/13/21	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.


Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 01/22/21	Sr. Program Analyst, Electronic Records Manager

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.
- 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:

 Signed by Nalabandian, Garo on 01/29/21

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Mary A. Lamary, Office of the Chief Human Capital Officer (OCHCO)

Name of System: Talent Management System (TMS)

Date CSB received PIA for review:

January 05, 2021

Date CSB completed PIA review:

January 28, 2021

Noted Issues:

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

Signature/Date:



Signed by Nalabandian, Garo
on 01/29/21

Copies of this PIA will be provided to:

*Thomas G. Ashley, Jr.
Director
IT Services Development and Operations Division
Office of the Chief Information Officer*

*Jonathan R. Feibus
Chief Information Security Officer (CISO)
Office of the Chief Information Officer*