Privacy Impact Assessment for the VA IT System:

VA Talent Management System 2.0 Assessing VA Central Office

Human Resources Services Center (HCSC), Talent Development Solutions (TDS)

March 16, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Griselda Gallegos	Griselda.Gallegos@va.gov	512-326-6037
Information System Owner	Jeffrey L. Henry	Jeffrey.Henry@va.gov	847-274-1093

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The VA Talent Management System (TMS 2.0) is a web-based enterprise application for managing education and training records within the VA workforce. It serves as the main access point to training opportunities within the Department, as well as from external sources. The system also provides individual development planning, self-assessment, and competency gap identification capabilities used to support employee development. As the VA's system of record for education and training, TMS 2.0 provides training certification and compliance tracking for all VA staff and it supports multiple internal and external reporting requirements. TMS 2.0 is a critical business tool used to support VA's employee engagement initiatives and customer service improvement projects.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The Human Resources and Administration/Operations Security and Preparedness (HRA/OSP) Human Capital Services Center (HCSC) – 006H is the business owner of the VA Talent Management System (TMS) 2.0, a cloud-based enterprise application for managing education and training records within the VA workforce. It serves as the main access point to training opportunities within the Department, as well as from external sources. The system also provides individual development planning, self-assessment, and competency gap identification capabilities used to support employee development. As the VA's system of record for education and training, TMS 2.0 provides training certification and compliance tracking for all VA staff and it supports multiple internal and external reporting requirements. TMS 2.0 is a critical business tool for Human Capital Management (HXM) used to support VA's employee engagement initiatives, customer service improvement projects, employee and leadership development programs, and other initiatives. The system also supports the Department as the reporting tool for efforts such as the Continuous Readiness in Information Security Program (CRISP), Enterprise Human Resources Integration (EHRI) reporting, volunteer preparedness training for the Disaster Emergency Medical Personnel System (DEMPS), and compliance with Health Insurance Portability and Accountability Act training requirements.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

TMS 2.0 provides capabilities and services to provide the management of Learning, Assignments, Content and Reporting for the Department of Veterans Affairs. TMS 2.0 also supports additional performance modules to enhance the existing talent management capabilities. The project will provide continuous support and maintenance for the items listed below that are in place, being developed for deployment, or deployed because of this project:

- VA customizations/extensions
- Integrations
- Connectors
- Supporting scripts
- Reports
- Configurations

Additionally, the project supports iContent hosting and support for 4,500 online courses available for 700,000 HXM Suite users (20,000 concurrent) in a cloud-based hosting environment. The project also provides license management, iContent courseware.

C. Indicate the ownership or control of the IT system or project.
VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

TMS 2.0 provides training certification and compliance tracking for 700,000 VA Employees and non-Employee staff (Contractors, Health Professional Trainees, Interns, Students, Without Compensation (WOC), Veterans Service Officers (VSO), State Employees, Department of Defense, Volunteers and Office of General Counsel (OIG))

E. A general description of the information in the IT system and the purpose for collecting this information.

TMS receives data from Identity Access Management (IAM) Single Sign-On (Internal) and receives data for the purpose of tracking training certification and compliance tracking from:
HR*SMART; Personnel and Accounting Integrated Data System (PAID);
Identity Access Management (IAM) Provisioning.
Education Data Repository (EDR);
Training and Performance Support System/Courseware Delivery System (TPSS/CDS), VBA Reporting Database.
VBA Reporting Database

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
HR*SMART; Personnel and Accounting Integrated Data System (PAID, Identity Access Management (IAM) Provisioning.); User demographic information (including PII)
Education Data Repository (EDR); Ensure the consistency of data within the TMS 2.0 database through the records synchronization
Training and Performance Support System/Courseware Delivery System (TPSS/CDS), VBA Reporting Database; Support VBA education and workforce analytics efforts

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

TMS 2.0 is hosted on Amazon Web Services (AWS) GovCLOUD and managed by SAPNS2 in a FEDRAMP certified environment.
hPII data that is sent to the TMS is kept in an encrypted Private Data Table (PDT) and not available for from the TMS User Interface.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The authority for maintenance of the System includes the following with any revisions or amendments: 5

U.S.C. 4103, 4115, and 4118 and Executive Orders 13478, 9830, 12107 as noted in Office of Personnel Management (OPM) Government-1, General Personnel Records system of record notice; 38 U.S.C. 501(a), 7406(c)(1) and 7802 as noted in Department of Veterans Affairs 76VA05 General Personnel Records (Title 38) system of records notice; Executive Order 11348, Providing for the Further Training of Government Employees; E-Government Act of 2002 (Public Law 107-347); Executive Order 12196 and 5 U.S.C. chapters 11 and 79 as noted in OPM Government-10, Employee Medical File System Records; Executive Order 12564; Urgent Relief for the Homeless Supplemental Appropriations Act of 1987, Pub. L. No. 100-71, Section 503, 101 Stat. 468 (1987); and Title 38, United States Code, Chapter 3, Section 210(c)(1,); Chapter 73, Section 4108 and Chapter 75, Section 4202 as noted in Employee

Medical File System of Records (Title 38)-VA: Published Prior to 1995, 08VA05; and, Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

Not at this time.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

Not at this time.

K. Whether the completion of this PIA could potentially result in technology changes

Not at this time.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

Additional Information Collected:

Person Identifier; Competency Assessment; Employee Number; Windows Log-On; Individual Development Plan; Service Computation Date; Learning History; Employee Human Resource Integration (EHRI) E-Profile Identifier; Student Identifier; TMS User Identifier; Learning History; Veteran Status; Comments about Student; Travel Card; VAU Identifier; Purchase Card

PII Mapping of Components (Servers/Database)

Talent Management System 2.0 consists of 1 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Talent Management System 2.0 and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Education Data Repository (EDR)	Yes	Yes	User demographics – Social Security Number, Date of Birth, UserID	Ensuring uniqueness of records in the application for data quality and reporting to accrediting bodies.	Hyper Text Transfer Protocol (HTTP) with Secure Sockets Layer (SSL) at the point of collection and storing of these data points in an encrypted data table that cannot be accessed via the application interface. Employee profiles are either directly sourced from HR system of record or manually entered

					through a web-interface inside the VA firewall. Data is communicated to TMS 2.0 via Secure File Transfer Protocol (SFTP) and then stored in the encrypted data table that cannot be accessed via the application interface. Least privilege principle is applied when granting administrative access to TMS 2.0 where this data can be viewed in via the application interface.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

- HR*SMART; Personnel and Accounting Integrated Data System (PAID); Identity Access Management (IAM) Single Sign-On (Internal); Identity Access Management (IAM) Provisioning

- Education Data Repository (EDR) – EDR is an internal database used to manage user demographic, training, and learning history data outside of TMS 2.0. EDR is hosted inside the VA firewall at the AITC.
- Blackboard – Blackboard is a third-party virtual learning environment used to offer facilitated, instructor-led, virtual classes. Blackboard stores user profile data and returns completion (learning history) records to TMS 2.0.

- Laerdal – Laerdal RQI is a third-party application used to offer clinical content. Laerdal stores user profile data and returns completion (learning history) records to TMS 2.0.

- Training and Performance Support System/Courseware Delivery System (TPSS/CDS) – TPSS/CDS is an application owned by the Veterans Benefits Administration (VBA) to deliver and track completion of VBA-specific content. TPSS/CDS is hosted inside the VA firewall at the Philadelphia Information Technology Center (PITC). TPSS/CDS stores user profile data and returns completion (learning history) records to TMS 2.0.

- Office of Personnel Management - Enterprise Human Resources Integration (EHRI)– Supports the internal efficiency and effectiveness of the Federal Government by streamlining and automating the exchange of Federal Employee Human Resource information.

- For non-VA employees, user profile data is collected directly from the individual through the TMS 2.0 self-enrollment module (which consists of an online web form: https://www.tms.va.gov/learning/user/Self RegistrationUserSelection.do).

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information from these sources is required to ensure uniqueness of records in the application for data quality and reporting to accrediting bodies.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Reports are created using information obtained from connectors, integrations, Administrators and Users.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

User Account data which contains demographic information used to manage user training and

development needs is collected through the following means:

1. TMS 2.0 Self-Enrollment Module: Non-VA employees directly create a user account using the web form (https://www.tms.va.gov/learning/user/Self RegistrationUserSelection.do) located on the TMS 2.0 Homepage.
2. VA Payroll Systems: User accounts for VA employees are created through data feeds from Personnel and Accounting Integrated Data (PAID) and HR SMART systems.
3. Education Data Repository (EDR): User accounts (both VA and Non-VA employees) are created and maintained through data feeds from the EDR. Nightly synchronization of user profile data between the EDR and TMS 2.0 is supported by automated processes.
4. Direct TMS 2.0 interface profile access: All TMS 2.0 users can directly create and update certain data fields with their user account using the profile functionality with TMS 2.0 interface.
5. Profile Maintenance: Provisioned TMS 2.0 Administrators can create and manage TMS 2.0 user accounts using the EDR web interface. The Profile Maintenance interconnection to TMS 2.0 is a web services Application Program Interface (API) and enables real-time user profile creation and updates to provision administrators.
6. Identity Access Management (IAM) Provisioning: Used to create and manage TMS 2.0 user profiles as new VA Staff are being On-Boarded and Off-Boarded to the VA.

Learning History data which provides the record of completed work is collected through the following means:

1. Individual manually records completion information, including grades or scores, to populate their learning history.
2. Learning history is automatically recorded by the content a user "completes" using common content communication standards or proprietary methods designed for the TMS 2.0.
3. TMS 2.0 administrators can manually record completions for users within their role of responsibility.
4. Through interfaces (web service APIs, Secure File Transfer Protocol (SFTP) flat file feeds, customized TMS 2.0 connectors), and using content communication standards with other content systems (CDS/TPSS, Blackboard, Laerdal, iContent) completions can be uploaded into the TMS 2.0 when matching unique identifiers for the records are available and an Interconnection Security Agreement (ISA) isin place.

Competency Assessment and Individual Development Plan data is collected through the following means:

1. Individual manually enters the data.
2. The individual's supervisor or other authorized official manually enters data.

Performance Review data is collected through the following means:

1. The individual manually enters the data
2. The individual's supervisor, rater of record or other authorized official manually enters data

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

TMS data is not collected on a form

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Routine daily automated processes are used as a quality control measure to maintain accurate and unique profiles in the TMS 2.0 system so that VA may reliably deliver training compliance reports. Discrepancies are resolved through the data cleansing actions of TMS 2.0 Administrators.
TMS 2.0 data accuracy is validated in four different ways:

TMS 2.0 employee profile data is sourced from our HR system(s) –HR-SMART;
Users are responsible for the accuracy of specific data elements for which there is no existing data source;
TMS 2.0 administrators (over 13,000) manage data of all sorts in the system in our decentralized model; and
Regular backend scripts and quality control audits that identify issues and, in some cases, resolve them automatically.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Monthly data quality audits using elements of Lean Six Sigma (LSS) analysis began in June 2015 to measure and monitor the level of "accurate and unique" user profile records in TMS 2.0.
The following data quality goals are the current focus areas for TMS 2.0 audits:

1. Establish and maintain accurate user email addresses in the TMS 2.0 system.
2. Establish unique user email addresses within TMS 2.0 user profiles.

3. Establish unique Person IDs within TMS 2.0 user profiles to eliminate duplicate profiles.
4. Establish accurate Org codes for TMS 2.0 User Profiles.
5. Establish acceptable lifecycle times for profiles created in MSE and kept in self-domain.
6. Eliminate user profiles created in MSE and left in self-domain for VA employees.
7. Establish and maintain accurate Supervisor/Manager information within TMS 2.0 user profiles.

A series of data quality audits can provide measurable inputs to benchmark targeted process and data improvement areas. The data quality audit measurements will serve to prioritize issues and incrementally bridge the deficiency gaps by embedding quality assurance into processes to achieve an enhanced future state.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The following is a full list of related laws, regulations and policies and the legal authorities:
Executive Order 11348, Providing for the Further Training of Government Employees
Executive Order 13111, Using Technology to Improve Training Technologies for Federal Government Employees
Executive Order 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers
Executive Order 12107, Relating to the Civil Service Commission and Labor-Management in the Federal Service
Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing
Executive Order 12196, Occupational Safety and Health Program for Federal Employees
Title III, Section 301, Subchapter III of Public Law 107-347 (Federal Information Security Management Act of 2002)
Title 38 of the U.S. Code Section 7406(c)(1)
Title 5 of the U.S. Code Sections 4103, 4115, and 4118
5 U.S.C. chapters 11, and 79
5 U.S.C. 552, "Freedom of Information Act," c. 1967
5 U.S.C. 552a, "Privacy Act," c. 1974
OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) Federal Information Security Management Act (FISMA) of 2002
OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002
VA Directive and Handbook 6502, Privacy Program
Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) between VA and OPM

Inter-Agency Agreement (IAA) between the VA and OPM

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

<u>Principle of Purpose Specification:</u> Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: TMS 2.0 collects a large amount of personally identifiable information (PII) to include the Social Security Number (SSN). Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: Human Capital Services Center (HCSC), Talent Development Solutions (TDS) team employs a variety of security measures 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, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management. These security and privacy requirements are government by Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) and Interagency Agreement (IAA) with the Office of Personnel Management and Department of Defense (DoD). For internal management of PII data, HCSC has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

HCSC TDS is also exploring way to minimize the amount of PII collected and maintained by TMS 2.0. HCSC TDS is working to integrate with VA's Provisioning System. This integration will result in the creation of a separate and unique user identification number which could be used instead of the SSN and/or TMS 2.0 User ID.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

Name – Multiple uses, including:
Display on a user's screen and on a supervisor's screen
Display on a training certificate of completion
Display on training and employee development related reports
Exchange with other systems with which TMS 2.0 has approved integrations
Differentiating one user record from another.

Social Security Number – Not visible through the TMS 2.0 interface. Used by back-end processes to uniquely identify user records during:
Self-enrollment profile creation
EHRI reporting
Integration with approved VA and third-party systems

Date of Birth – Not visible through the TMS 2.0 interface. Used by back-end processes to support
Self-enrollment
EHRI reporting
Accreditation reporting

Business Mailing Address – For delivery of hard-copy training materials.

Business Zip Code – Delivery of hard-copy training materials.

Phone Number(s) – Contacting individuals with respect to talent management system processes.

Email Address – For non-employees, this is a user profile identifier. Other uses fall in the category of notifying individuals with respect to multiple talent management system processes:
Learning expiration
Learning assignment
Learning scheduling
System approval actions

Ad hoc communications regarding talent management topics
Administrator notifications

Financial Account Information- Collected for senior executives only in order to facilitate the succession planning process.

Certificate/License Numbers - Support recording and reporting of accredited learning.

Competency Assessments - Supports identification of an individual's skills and sill gaps, the latter of which is used to support creation of individual development plans.

Individual Development Plan – Assist employees in career and personal development.

Learning History – Provide official record of training activities.

Veteran Status – Supports senior executive succession planning efforts.

Employee Number – Unique user identifier that can validate user identities when integrating with other VA systems.

Service Computation Date – Informs assignment and recurrence of training.

Student Identifier – Application-specific unique identifier for the user that is used for:
System login/unique identifier
Integration with other VA and third-party systems
Included in report outputs (can be masked)

Comments about Student – Document actions taken to update a user's profile.

Person Identifier- Unique identifier for a user that supports integration with other systems.

Windows Log On – Aids in TMS 2.0 administrator identification of users. Can also be included in report outputs for the same purpose. Also used by Information Security Officers and local administrators to identify users' compliance with mandatory training requirements.

Travel Card – Alpha character used only to determine if an individual holds a government travel card and, if so, what level of training their travel card status requires.

Purchase Card – Alpha character used only to determine if an individual holds a government purchase card and, if so, what level of training their purchase card status requires.

VAU Identifier – Used to uniquely identify a user in support of VA's Single Sign-On capability.

E-Profile Identifier – Used to support a pharmacist's accreditation documentation requirements.

VA Security ID – Used to uniquely identify user profiles and facilitate VA Single Sign-On

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Although the system does not inherently provide such functionality, the supporting TMS 2.0 relational database could be accessed to perform aggregating analysis using reporting tools. These capabilities are only available to provisioned

TMS 2.0 administrators through the system's administrator interface (https://www.tms.va.gov/learning/admin/login.jsp).

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

TMS 2.0 will place any new or previously unutilized information about an individual in the individual's existing record.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

The solution is housed in a FedRAMP-authorized cloud hosting environment. Data that is considered PII is not displayed through the user interface or on reports. TMS 2.0 data that contains PII is encrypted when transmitted.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The solution is housed in a FedRAMP-authorized cloud hosting environment.

There are Standard Roles configured consistently across all Domains, as well as a single System Level Manager, which is used to manage the TMS 2.0 at an enterprise level. All Roles require basic TMS Administrator skills. Access to TMS 2.0 functions is restricted by these Roles which are managed under the concept of 'Least Privilege' restricting access to TMS 2.0 data to the minimum necessary to perform a business function.

Social security numbers and dates of birth are maintained in an encrypted Private Data Table (PDT) that is not accessible from the TMS 2.0 user interface. PDT data is collected solely for the purposes of uniquely identifying users for database management and reporting purposes.

TMS 2.0 Standard Roles include:

- Domain Manager (DM) – The Domain Manager is responsible for managing all Admin accounts within the Domain (apart from giving out the DM role itself). The Domain Manager role is an Add-on role which MUST be assigned along with the Learning Manager role. There should be a primary and back-up Domain Manager identified for each Domain.
- User Manager (UM) – The User Manager can manage Catalogs, Proctor codes, and Users within the Domain. They also can merge User accounts and assign Approval Roles to Users. The User Manager Role is an Add-on role with MUST be assigned along with the Learning Manager role.

- Learning Manager (LM) - The Learning Manager is primarily responsible for managing and tracking User training needs. They have access to create Items and Scheduled Offerings and to record learning for Users. They can also provide enhanced access to Users who are also Instructors within the TMS and manage Programs. The LM can perform all the functions of the IM, RM, SM, AM, HD and PR.
- Item Manager (IM) - The Item Manager is primarily responsible for creating/managing Items and Curriculum, to include placing them in Catalogs. The IM can also create Direct Links, manage Programs, and run reports.
- Registration Manager (RM) - The Registration Manager is primarily responsible for registering Users in Scheduled Offerings and recording learning. The RM can also edit Scheduled Offerings and Classes, manage Slots, and run reports.
- Scheduling Manager (SM) - The Scheduling Manager is primarily responsible for creating and managing Scheduled Offerings – to include managing Slots and the registration of Users. The SM can also create Direct Links, manage Classes and Instructors, and run reports.
- Assignment Manager (AM) - The Assignment Manager is primarily responsible for managing learning assignments of Users. The AM can also manage Classes, manage Slots, and run reports.
- Assignment Profile Manager (APM) - The Assignment Profile Manager is primarily responsible for creating/managing Assignment Profiles. This is an add-on Role and must be added in conjunction with another Admin Role, typically LM.
- Help Desk Manager (HD) - The Help Desk Manager is primarily responsible for providing initial support for TMS Users, such as viewing the User Learning History and login. The HD role can also Edit Accreditation Types and Occupational Categories for Users.
- Question and Exam Manager (QEM) – The Question and Exam Manager can create Objectives, Questions, and Exam Objects. The QEM can also create and manage Questionnaire/Surveys. This is an add-on Role and must be added in conjunction with another Admin Role.
- Report Manager (RPT) – The Report Manager Role is given to those whose only administrative function in the TMS is the running of Reports. They may not have access to all reports.
- Ad-Hoc Notifications Manager (AHN) – The Ad-Hoc Notifications Manager can send ad- hoc email notifications to Users within their Domain. This is an add-on Role and must be added in conjunction with another Admin Role.
- Managed Self Enrollment Manager (MSE) – The Managed Self Enrollment Manager can search for, view, and validate self-enrolled Users.
- Learning History Import Manager (LHIM) – The Learning History Import Manager can import Learning History (generally created by the Bar Code Scanning utility). This is an add-on Role and must be added in conjunction with another Admin Role.
- ISO (Information Security Officer) – The ISO Role allows for view access only for User accounts. It is assigned to Information Security Officers so that they can view the status of CRISP training for Users Enterprise-wide.
- Catalog Manager (CTLGM) – The Catalog Manager, limited to Administration Level Domains, can set a Search Tier and Search Weight on Catalogs added to Items. This is an add-on Role and must be added in conjunction with another Admin Role, typically LM or IM.
- Competency Manager (CM) – The Competency Manager can manage Competencies associated with Items and Programs within their Domains. This is an add-on Role and must be added in conjunction with another Admin Role, typically LM.
- Accreditation Manager (ACM) – The Accreditation Manager can add Accreditations, based on nationally entered Accreditation Types, to their Domain. ACM can also Edit Accreditation Types and Occupational Categories for Users. This is an add-on Role and must be added in conjunction with another Admin Role, typically LM.

- Accreditation Item Manager (ACIM) – The Accreditation Item Manager can associate Accreditations with Items within their Domain. This is an add-on Role and must be added in conjunction with another Admin Role, typically LM.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

PII data is either encrypted (e.g., SSN) or masked (e.g., Legacy TMS UserID's with partial DoB). Access to the data is restricted by business need to a Role that allows viewing or reporting on fields that contain PII. SSN's are stored encrypted and are only used for machine to machine data matching. They cannot be viewed or used in a report on TMS 2.0.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project? This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The assignment of TMS 2.0 administrator roles is inconsistent. This may lead to inappropriate access to, or modification of, TMS 2.0 information making compliance reports inaccurate. Business and personnel decisions may be made based upon these inaccurate compliance reports. The Privacy Act requires agencies to make reasonable efforts to ensure information contained in a system of records is accurate, relevant, timely and complete.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

TMS 2.0 management restricts the granting of the role that allows local TMS 2.0 administrators to create and assign responsibilities to lower-level TMS 2.0 administrators. This returns oversight control to the Department level of who can grant access to TMS 2.0 data. TMS 2.0 Administrators are required to complete role-based training for various levels of administration, all users are required to sign Rules of Behavior as part of their security awareness and privacy training. Standardized TMS
2.0 Administrator privileging rules have been established and supported, as well as auditing logs and procedures put in place to ensure consistent implementation.

2.4c Does access require manager approval?

Access requires manager approval.

2.4d Is access to the PII being monitored, tracked, or recorded?

Access to PII is provided by Roles. Roles are granted based on business need and restricted by organization. There are audit reports at the organizational level to monitor assigned roles and assessing the business need for the roles.

2.4e Who is responsible for assuring safeguards for the PII?

The Talent Development Solutions TMS Systems Management team is responsible for ensuring PII data is encrypted, not displayed or masked. Each VA Organization is responsible for ensuring that only users who have completed FISMA and Privacy training and have a business need for the data have access to masked PII data.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

- Name
- Social Security Number
- Date of Birth
- Business Mailing Address
- Business Zip Code
- Financial Account Information
- Phone Number (s)
- Email Address
- Individual Development Plan
- Certificate/License Number
- Competency Assessment
- Employee Number
- Learning History
- Veteran Status
- Comments about Student
- Service computation Date
- Student Identifier
- Travel Card

- Person Identifier
- Windows Log On
- VAU Identifier
- Purchase Card
- Employee Human Resource Integration (EHRI) E-Profile Identifier
- VA Security ID (SECID)

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

As a preliminary matter, General Records Schedule 2.6, Employee Training Records, for training records applies and learning history retention requirements established by providers for accredited training and General Records Control Schedule 2.7. However, all records are considered permanent until a full evaluation by the VA Records Management Officer is identified and conducts an evaluation.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, all records are approved and considered permanent until full evaluation is complete.

3.3b Please indicate each records retention schedule, series, and disposition authority.

The records generated in the process of providing education, training, and guidance to Privacy and FOIA Officers and Records Managers on compliance monitoring and preparation for PCA Performance Audits. Educational topics include the importance of a compliant monitoring program, how to set up a compliant monitoring program and providing sample tools and SOPs to use. Some training may be in direct response to issues found either by the White House Office of Special Council, VA Office of Inspector General (OIG), HHS or other Agencies tasked with compliance monitoring or investigating complaints. Item Number: 1008.5, Deposition Authority: DAA-0015-2017-0002- 0006, https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Currently, all records are considered permanent until a full evaluation is complete. However, TMS 2.0 will follow standard VA destruction procedures for the elimination of SPI (see details below). Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014). http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

When required, this data is deleted from the file location and then permanently deleted from the deleted item's location or recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1.

Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII is not used for the purposes of research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it

needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by the Talent Management System will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: TMS 2.0 inactive records were archived in 2018. This will provide greater detail for the retention and disposal schedules. All records are considered permanent until officially evaluated. This policy ensures no federal records that might require NARA archiving are destroyed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
HR*SMART; Personnel and Accounting Integrated Data System (PAID); Identity Access Management (IAM) Single Sign-On (Internal); Identity Access Management (IAM) Provisioning	User demographic information (including PII)	User demographics - SSN, DoB, TMSUserID, SecurityID, Name, email address, NTLogin, SupervisorID; VA UID; HR*Smart EIN; Pay Grade; Pay Step	Secure File Transfer Protocol (SFTP) after storage in an internal database (Personnel and Accounting Integrated Data System (PAID) & HRSMART); Security Assertion Markup Language (SAML) insertion (Single Sign-On Integration (SSOi)); Web Service Application Program Interface (API) (Provisioning)
Education Data Repository (EDR)	Ensure the consistency of data within the TMS 2.0 database through the records synchronization	User demographics: SSN, DoB, TMSUserID, SecurityID, PersonID, Name, email address, NTLogin, SupervisorID; Phone Number, Mobile Number; Username; VA UID; HR*Smart EIN; Pay Grade; Pay Step; Training	Secure File Transfer Protocol (SFTP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		completions – PersonID; Content metadata – No PII/PHI; and Evaluation responses – PersonID.	
Training and Performance Support System/Courseware Delivery System (TPSS/CDS); VBA Reporting Database	Support VBA education and workforce analytics efforts	Training completions status - TMSUserID; Training assignments - TMSUserID; User profile information – TMSUserID, Name, PersonID; Organizational data – No PII/PHI.	Secure File Transfer Protocol (SFTP); Web Services Application Program Interface (API); Content Communications Standards

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

Office of Personnel Management	Support the internal efficiency and effectiveness of the Federal Government by streamlining and automating the exchange of Federal employee HR information	SSN, Organization, Learning History	OPM GOVT -1; MOU/ISA	Secure FTP
Blackboard, Inc.	Support VA learning and employee development business requirements	UserID, Name, email address, Learning History	OPM GOVT-1 – Routine Use A; MOU/ISA	Secure FTP
Laerdal	Support the management of training related to VHA's Basic and Advanced Cardiac Life Support program	UserID, Name, email address, Learning History	OPM GOVT-1 – Routine Use A; MOU/ISA	Secure FTP

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification(PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized for the system. Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU) are kept current and monitored closely to ensure protection of information.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The following VA System of Record Notices (SORNs) which are published in the Federal Register and available online applies to the Talent Management System (TMS 2.0):

- OPM Government-1, General Personnel Records: http://www.gpo.gov/fdsys/pkg/FR-2006-06- 19/html/06-5459.htm

- 76VA05 General Personnel Records (Title 38): http://www.gpo.gov/fdsys/pkg/FR-2000-07- 20/pdf/00-18287.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Authority: The Department of Veterans Affairs (VA) is authorized to collect this information under the authority of Executive Order 9397 as amended by Executive Order 13478; Title III, Section 301, Subchapter III of Public Law 107-347 (Federal Information Security Management Act of 2002); Section 7406(c)(1) of Title 38 of the U.S. Code; and Sections 4103, 4115, and 4118 of Title 5 of the U.S. Code Version Date: October 1, 2022.

Purpose: The Department of Veterans Affairs (VA) will use this information to ensure your training records are properly documented and retained into one system, the VA Talent Management System (TMS); and accurately credited to your TMS profile to acknowledge and provide verification training requirements are met.

Routine Uses: This information will be used by and disclosed to VA personnel and contractors who need the information to assist with activities related to the training management purposes. Additionally, this information will become a part of your permanent personnel record and is included in the respective government-wide, OPM/GOVT-1 – General Personnel Records (71 FR35356) and VA-specific, 76VA05 General Personnel Records -Title 38 (65 FR 45131) electronic system of records notices (SORNs), and is subject to all published routine uses within these SORNs.

Disclosure: Furnishing this information is voluntary, including Social Security Number; however, failure to furnish the requested information may prevent you from establishing a TMS profile and delay the completion of training that would be assigned as a result of the completion of this form.

Social Security Number (SSN): Your SSN may be requested under the authority of Executive Order 9397 as amended by Executive Order 13478. The SSN is used as a unique identifier to ensure that each individual's record in the system is unique, complete and accurate and the information is properly attributed. The SSN is not used by, nor displayed in, the TMS for any other purpose.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Privacy Act Statement(s) are also provided on the web forms used to facilitate the TMS 2.0 managed self- enrollment process and general profile maintenance.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

An individual may decline to provide information; however, if certain information is not provided, the individual may not receive credit for completing mandatory and optional trainings. Completion of certain mandatory trainings such as the privacy and information security awareness training is required by federal mandates and VA policy (e.g. Directive 6500, Managing Information Security Risk: VA Information Security Program), prior to an individual gaining access to VA IT systems or VA sensitive information and must be documented in TMS 2.0 (as the official VA system of records

for training records) for internal and Inspector General audits. If an individual decline to provide the information required to obtain a TMS 2.0 account, they may not be able to perform job functions or contractual obligations – due to the lack of an official training record demonstrating the completion of mandatory training.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Consent to particular uses is defined in the notice given in the SORNs applicable to TMS 2.0 (see: question 6.1) and this PIA. Any uses outside that defined scope would require additional notice and consent; however, expansion is not unforeseen.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that individuals may not receive notice that their information is being collected maintained, or disclosed by HCSC TDS prior to providing the information to VA.

Mitigation: Employees and contractors are on notice upon entering VA service that certain training may be required of them, and, as part of that training certain information may be required. It is important to note that the information provided is the same information already provided at hiring or security clearance. All other users are provided notice through the Privacy Act notices detailed in Appendix A. Additional mitigation is provided by making the System of Record Notices (SORNs) and this Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

All users must enter authentication information (username/password or personal identity verification (PIV) and personal identification number (PIN)) to gain access to their information. Individuals may personally ensure that all of their user profile information is accurate and can directly make changes to portions of this information. If an individual feels the un-editable portions of their individual demographics, or any of their training information is inaccurate, a TMS 2.0 Administrator is required to verify and make appropriate changes either in the TMS 2.0 or in the data source (e.g., HR system of record).

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

TMS 2.0 is not exempt from the provisions of the Privacy Act

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

TMS User profiles are created by the following means:

(1) Automatically from a HRSmart data feed
(2) Automatically from a IAM/Provisioning web service
(3) Manually from a Profile Maintenance (PM) Admin
(4) Manually by a non-Employee using Managed Self Enrollment (MSE)

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Users must notify their supervisor, Human Resources, respective TMS 2.0 Administrator or the TMS

2.0 help desk to correct erroneous information. Individuals may also directly update in the TMS 2.0 certain data elements of their user profile including, contact information, employee information, travel preferences, accreditations, occupational category, language skills, groups and associations, external work history, projects, awards, professional licenses/certifications and education.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Users are provided this information through direct contact with their supervisor and/or TMS 2.0 Administrator via email, phone and/or face-to face communication. There is also readily available documentation, such as the TMS 2.0 User Guide and embedded help functions within TMS 2.0, which contain standard operating procedures that individuals can use to make correction via direct access to the system.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Users may always contact their supervisor, TMS 2.0 Administrator and/or the TMS 2.0 help desk for assistance in correcting whatever issue they may encounter.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals may not receive notification of the procedures on how to correct or access their information maintained in TMS 2.0.

Mitigation: Procedural mechanisms for access and correction are included within TMS 2.0 and available as needed via an individual's supervisor or TMS 2.0 Administrator. Notice is also given on the websites associated with TMS 2.0 training as well as in the Federal Register pursuance to the Privacy Act as well as this PIA.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

User access to TMS 2.0 falls in three general categories: 1) End users (e.g. - VA employees, contractors, interns, volunteers, etc.) and their supervisors, 2) TMS 2.0 Administrator users (e.g. Domain Managers, Learning Mangers, Item Managers, etc.), and (3) System Administrators (e.g. database administrators, network engineers, etc.).

End users (employees, contractors) are granted access to TMS 2.0 in one of four ways:

1. Through an automated data feed from the HRSmart Human Resources system. If the VA employeehas an active record in the HR Smart system and that record has been imported to TMS 2.0 via an HR Connector, providing the employee access to TMS 2.0. Likewise, if the VA employee has an active record in TMS 2.0 and leaves the government, their account will be deactivated via an automated process during the next data upload from HR Smart. This method is primarily designated for VA employees.

2. Through the managed self-enrollment (MSE) process. The end user submits an electronic form located on the TMS 2.0 website and an account is created allowing limited access to TMS 2.0 to complete mandatory privacy and information security awareness trainings or to register for VA sponsored trainings or conferences. This method is designated for users that are not managed by HRSmart.
3. End user accounts can also be activated/ deactivated by a TMS 2.0 Administrator with the

appropriate permissions.

4. Profiles for VA Staff that are being On-Boarded or Off-Boarded by the VA Access Identify Management (IAM) Provisioning team are automatically added (or separated) from the TMS 2.0.

   End user access procedures are documented in job aids that are readily available on internal and external VA web sites, as well as via direct distribution from the individual user's VA point of contact (i.e., supervisor, TMS 2.0 administrator, Contracting Officer's Representative, etc.).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Access to TMS 2.0 is provided by Roles. Users from other agencies will need to demonstrate a business need to be provided a role that has access to PII. Users from DoD and other Federal Agencies are provided TMS User profiles and provided access by VA Organizations that they are providing support or services for.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

There are 31 TMS 2.0 Administrator functional roles (see Appendix C – Talent Management System Administrator Roles and Workflows for a high-level overview of system privileges assigned to each role). The functional roles are configured at the Department-level and assigned in a decentralized manner by TMS 2.0 Administrators assigned the functional role of Domain Manager. Domain Managers are required to take role-specific training to ensure functional roles are assigned appropriately to the TMS 2.0 Administrators within their area of responsibility (or Domain). Domain access and administrative roles are configured in the system according to the business requirements set forth by the Domain Manager and VA System Owner.

TMS 2.0 Administrator access procedures are documented in job aids and training materials that are readily available on internal and external VA web sites, community of practice sites, as well as via direct distribution from the TMS 2.0 Help Desk, other TMS 2.0 administrators, and the TDS staff.

System Administrators (database administrators, network engineers) are employees and contractors of VA that are responsible for the actual software and hardware on which the TMS 2.0 operates. Personnel having system level access to TMS 2.0 must first submit a background investigation and go through the government clearance process according to the VA Directive 0710, Personnel Security and Suitability Program. There are over-arching TMS 2.0 Administrator Roles available to this cohort that provide broader access to the system configuration controls and application settings. These roles are not widely distributed.

System Administrator access procedures are documented in the TMS 2.0 Enterprise Solution Design Document.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business

Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes – Contractors will have access to TMS 2.0 after completing mandatory and assigned trainings. Contractors accessing TMS 2.0 are required to undergo a background investigation and public trust clearance, but often contract terms require access to TMS 2.0 before receiving a public trust clearance. Each respective VA Program Manager and Contracting Officer Representative is responsible for working with their TMS 2.0 Administrator to monitor contractors' access to TMS 2.0.

Additionally, provisioned TMS 2.0 contractors provide system administration support which includes conducting quality assurance, IT security analysis, database management, user helpdesk technical support and incident reporting support. All TMS 2.0 contractors providing system administration support are required to undergo a background investigation and receive a public trust clearance prior to being granted system administration access. TMS 2.0 Program Managers and Contracting Officer Representatives review TMS 2.0 system administration and support contracts, annually.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

All individuals (employees, contractors, interns, volunteers, etc.) who have access to or use VA IT systems or VA sensitive information must complete the federally mandated Privacy and Information Security Awareness training and sign the VA National Rules of Behavior. Additionally, TMS 2.0 Administrators are required to complete specific role-based trainings that includes specific instruction on how to appropriately handle information (including, sensitive information) maintained in TMS 2.0. HIPAA Awareness training is included in the mandated Privacy and Security Awareness training that is a requirement for all users to complete. VA Privacy and HIPAA training is automatically assigned to employees with Occupation Codes or Organization Codes identified by the VHA Privacy Office or to users who have been identified by their manager of having access to PHI information.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* August 25, 2020
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* January 28, 2021
5. *The Authorization Termination Date:* November 5, 2023
6. *The Risk Review Completion Date:* January 22, 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Yes – The Authority to Operate was granted on January 28, 2021. The current FIPS 199 Classification of the Talent Management System 2.0 is Moderate.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, the TMS 2.0 is hosted on AWS GovCloud and is FEDRAMP authorized. Technical details on the interconnection is established and maintained within the Interconnection Security Agreement (ISA). The ISA used to formally document the reasons, methodology and approvals for interconnecting IT systems; to identify the basic document the basic components of the interconnection; to identify methods and levels of interconnectivity and to document potential security risks associated with the interconnection.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes, the Department of Veterans Affairs UTILIZES A Memorandum of Understanding (MOU) to document the terms and conditions for sharing data and information resources in a secure manner.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No, there is not a provision for ancillary data to be collected.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

TMS 2.0 is managed by AWS GovCloud and Akamai Content Delivery Services are FedRAMP Joint Authorization Board (JAB)

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.04.17 15:06:07 -04'00'

Privacy Officer, Tonya Facemire

Griselda Gallegos 204736

Digitally signed by Griselda Gallegos 204736
Date: 2023.04.17 11:03:53 -05'00'

Information Systems Security Officer, Griselda Gallegos

JEFFREY HENRY

Digitally signed by JEFFREY HENRY
Date: 2023.04.14 14:50:39 -05'00'

Information Systems Owner, Jeffrey L. Henry

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

Privacy Act Statement for TMS 2.0 Self-Enrolled Users:

Authority: The Department of Veterans Affairs (VA) is authorized to collect this information under the authority of Executive Order 9397 as amended by Executive Order 13478; Title III, Section 301, Subchapter III of Public Law 107-347 (Federal Information Security Management Act of 2002); Section 7406(c)(1) of Title 38 of the U.S. Code; and Sections 4103, 4115, and 4118 of Title 5 of the U.S. Code.

Purpose: The Department of Veterans Affairs (VA) will use this information to ensure your training records are properly documented and retained into one system, the VA Talent Management System (TMS 2.0); and, accurately credited to your TMS 2.0 profile to acknowledge and provide verification training requirements are met.

Routine Uses: This information will be used by and disclosed to VA personnel and contractors who need the information to assist with activities related to the training management purposes. Additionally, this information will become a part of your permanent personnel record and is included in the respective government-wide, OPM/GOVT-1 – General Personnel Records (71 FR35356) and VA-specific, 76VA05 General Personnel Records -Title 38 (65 FR 45131) electronic system of recordsnotices (SORNs), and is subject to all published routine uses within these SORNs.

Disclosure: Furnishing this information is voluntary, including Social Security Number; however, failure to furnish the requested information may prevent you from establishing a TMS 2.0 profile and delay the completion of training that would be assigned as a result of the completion of this form.

Social Security Number (SSN): Your SSN may be requested under the authority of Executive Order 9397 as amended by Executive Order 13478. The SSN is used as a unique identifier to ensure that each individual's record in the system is unique, complete and accurate and the information is properly attributed. The SSN is not used by, nor displayed in, the TMS 2.0 for any other purpose.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices