Privacy Impact Assessment for the VA IT System called:

Immersion Cloud: Altair Knowledge Hub/Datawatch

Veteran's Benefits Administration (VBA) Office of Financial Management (OFM)/Fiscal Systems Staff

Date PIA submitted for review:

January 11, 2021

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Simon Caines	Simon.Caines@va.gov	(202) 461-9468
Information System Security Officer (ISSO)	Mark McGee	James.McGee5@va.gov	520-629-4834
Information System Owner	Yolonda Reese	Yolonda.Reese2@va.gov	727-273-601

Abstract

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

Altair Knowledge Hub is a browser-based and team-oriented shared data exploration, preparation, automation, and distribution across organizations preparation tool. It automates the data extraction from a wide variety of data file formats and integrates that information with disparate database and reporting tools. Government users across mission areas from benefits to finance and operations to intelligence can use Immersion Cloud to centrally organize historical information, connect data repositories, and automate extraction, transformation, and reporting.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The IT system name is Immersion Cloud (also referenced as: Altair, Altair Knowledge Hub/Datawatch, Datawatch/Monarch Complete) and it is owned by the VBA Office of Financial Management (OFM)/Financial Management Business Solutions Staff. Altair Knowledge Hub/Datawatch will provide authorized users at VBA's Office of Financial Management (OFM) the ability to create and share reconciliation data models among OFM authorized users to eliminate the use of spreadsheets and manual data entry by extracting financial data trapped in portable document format (PDF) and core system reports and eliminate redundant processes through pre-built, shareable models to save time and increase data efficiency. Altair Knowledge Hub/Datawatch will be hosted in Amazon Web Services (AWS) GovCloud. Altair Knowledge Hub/Datawatch does not have any external connections, but will connect internally to other VA systems (Financial Accounting System, (FAS), Benefits Delivery Network (BDN), and Financial Management System (FMS)). The users upload data from their VA desktop, process the data, and then download the data again to their desktop.

It will process full names, Social Security Numbers (SSN), claim numbers, and payment amounts as it relates to the veteran benefit payments. This information is collected by VBA for the administration of all veteran benefit payments. This covers the entire population of veterans serviced by all 56 regional benefits offices. It does not explicitly include VHA/Hospitals or Clinics, but it is assumed they would have been serviced by the Regional Office (RO) to be entitled to health care. The Altair Knowledge Hub Software as a Service (SaaS) application is deployed in the already-authorized AWS GovCloud Platform as a Service (PaaS) and is pursuing full VA and FedRAMP ATOs. The risk is categorized as Moderate. Authority to use this system is granted by OMB Memorandum A-130. Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority to operate the benefit delivery systems. 38 U.S.C. §5106;5 U.S.C. §552a (b)(3);5 U.S.C. 552a(b)(3);20 CFR 401.150 provide the legal authority to use or collect SSNs in regard to Veterans' Benefits information, upon request, for purposes of determining eligibility or for amount of VA benefits, or verifying other information with respect thereto.

The system will be primarily used by VA Staff in addition to a few privileged Altair employees for administrative purposes, and all data input to the system will be stored offline, only the models produced by the system will be stored within the system. There will be five privileged "external" users from Immersion Cloud operating and maintaining the system. Further, there will be approximately 140 end users to Immersion Cloud and the Altair Knowledge Hub application. The 140 internal end users will be VA employees and contractors by 2021. All users are on a single site. The completion of this PIA and approval of the system will improve financial data analytics processes, eliminating the manual data entry process that is currently in place. No technology changes will surface as a result of the completion of this PIA. Ownership rights of the data – including PII - are outlined in a contract between the Cloud Service Provider, Immersion Consulting, and the VA. The CSP has no rights in the data, and the US Government maintains its right in the data loaded, processed, and downloaded from the system. The contract also states that Altair can hold VA information and PII given they have the appropriate security controls in place to protect that data, as outlined in VA Directive 6500.

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.

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 Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Other Unique Identifying Number (list below)

Claim numbers used as case identifiers (Used interchangeably with SSN as Claim number predates the use of SSN in VBA).

PII Mapping of Components

Immersion Cloud consists of four key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Immersion Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
Altair Knowledge Hub Application (Server)	Yes	Yes	Beneficiary Account Numbers. VA user email addresses	Beneficiary data used for financial reporting. VA user data used for Access Control.	Confidentiality: User privacy training. FIPS-140-2 validated encryption at rest and TLS v1.2 for data upload and download through browser session. Strong authentication and access control limit to those who need to know.
AWS GovCloud Storage and Backup (Services)	Yes	Yes	Financial Account Number, Beneficiary Account Numbers, SSN	Used for back-up and recovery of Immersion Cloud.	Confidentiality: User privacy training. FIPS-140-2 validated encryption at rest and TLS v1.2 for data upload and download through browser session. Strong authentication and access control limit to those who need to know.
Immersion Cloud Security and Operations GSS	No	No	N/A	N/A	GSS does not contain PII. GSS users may access PII if they have access to those components.

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Immersion Cloud will process data extracted from internal and independent systems managed by other Program Owners across VA and affiliated Departments and Agencies. This data was originally collected under the auspices of the Program Owner. While the reporting requirements and specific data elements have not yet been identified, the VBA OCFO expects the use of the system will include PII obtained by the source system owners. Services may include mortgage guarantees, education benefits, cemetery administration, disability compensation, etc.VA

Program Owners: may provide PII as part of agency-wide financial reporting requirement. The agency providing the information collects the PII in delivery of agency services and their related systems of record; the source system reports are utilized as inputs for this system. Services may include mortgage guarantees, education benefits, cemetery administration, disability compensation, etc.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Immersion Cloud does not directly receive information from external sources. VA users manually upload reports to the system and subsequently manually download the output through the Web user interface. VA users are expected to upload or enter information from financial reports obtained electronically from existing agency source systems (BDN, FAS, FMS). No data from these systems is directly uploaded to Altair, it is done manually by VA users.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

Altair Knowledge Hub is a browser-based and team-oriented shared data exploration, preparation, automation, and distribution across organizations preparation tool. It automates the data extraction from a wide variety of data file formats including Microsoft Excel spreadsheets, Adobe PDF documents, delimited files, XML, JSON, and integrates that information with disparate database and reporting tools.

Government users across mission areas from benefits to finance and operations to intelligence can use Immersion Cloud to centrally organize historical information, connect data repositories, and automate extraction, transformation, and reporting.

Reports containing detail accounting transactions, daily accounting journals, accounting journal trial balances, and General Ledger Trial Balances from the Benefit Delivery Network (BDN), Financial Accounting System (FAS) and Financial Management System (FMS) are reconciled for financial reporting including Fund Balance with Treasury.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The system assumes that the original source data was checked for accuracy when it was first entered into the source systems.
Immersion Cloud has been implemented as an automated data extraction system for diverse source reports to include .xlsx, .pdf, .csv, etc. There are three activities undertaken by agency to assure the accuracy of the data in the system:

1. When developing the initial extraction tool for the data on a set of given reports, organizational analysts review the accuracy of the reporting output using existing, hand-built models. The QA process establishes the expectations for system output.
2. While the tool is in use, organizational analysts will conduct output QA review to confirm the expected output.
3. When uploading the data, the extraction tool automatically alerts the operator (organizational analyst) when the input format has deviated from that expected. When there is an update to source information format, the analyst updates the extraction mechanism as well as the reporting module to achieve the desired output.

1.6 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 authority for this collection of information is based on:

Federal Information Security Modernization Act of 2014 (FISMA 2014)
VA Directive 6500, VA Directive 6500: VA Cybersecurity Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program
Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security
Office of Management and Budget (OMB) Circular A-130, Managing Information as Strategic Resource Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. Executive Order 9397 gives authority to collect and use the SSN as an identifier. Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority to operate the benefit delivery systems. 38 U.S.C. §5106;5 U.S.C. §552a (b)(3);5 U.S.C. 552a(b)(3);20 CFR 401.150 provide the legal authority to use or collect SSNs in regard to Veterans' Benefits information, upon request, for purposes of determining eligibility or for amount of VA benefits, or verifying other information with respect thereto.

The following SORNs also apply to this system:

SORN notice 13VA047, Individuals Submitting Invoices Vouchers for Payment and Accounting Transactional Data
https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf

17VA26/78 FR 71727; Loan Guaranty Fee Personnel and Program Participant Records
https://www.govinfo.gov/content/pkg/FR-2019-04-17/pdf/2019-07647.pdf

36VA29/83 FR 44407; Veterans and Uniformed Services Personnel Programs of US Government Life Insurance
https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf

37VA27/79 FR 41744 Beneficiary Fiduciary Field Systems
https://www.govinfo.gov/content/pkg/FR-2014-07-17/pdf/2014-16810.pdf

38VA21; Veterans and Beneficiaries Identification Records Location Subsystem
https://www.oprm.va.gov/docs/sorn/SORN38VA21.PDF

58VA21/22/28 84 FR 4138; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records
https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

88VA244/83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS)
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

137VA005Q/74 FR 37309; Veterans Information Solutions (VIS)
https://www.govinfo.gov/content/pkg/FR-2009-07-28/pdf/E9-17910.pdf

138VA005Q/74 FR 37093; Veterans Affairs/Department of Defense Identity Repository (VADIR)
https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

VA 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records
http://www.gpo.gov/fdsys/pkg/FR-2014-01-23/pdf/2014-01286.pdf

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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.

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

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

Principle of Minimization: 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: There is a risk that PII gets released outside of specified purpose.

Mitigation:

1. All VA users and Immersion Cloud security and operations team members must complete the VA Privacy and Security training according to agency requirements annually.

2. Data at rest is encrypted with a FIPS 140-2 validated encryption module.
3. Data transfer occurs using https encrypted with Transport Layer Security v1.2, FIPS 140-2 validated encryption module.
4. The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

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.

The PII information stored in Immersion Cloud will help increase efficiency for the teams that use it by automating data extraction from multiple formats into an automated data analytics tool, a process that has historically required data entry by hand. Reports can be generated quickly and more accurately than previously done, providing valuable time and information back into the hands of its users. Reports containing detail accounting transactions, daily accounting journals, accounting journal trial balances, and General Ledger Trial Balances from the Benefit Delivery Network (BDN), Financial Accounting System (FAS) and Financial Management System (FMS) are reconciled and used for financial reporting including Fund Balance with Treasury. All uses are for VBA internal.

Full name: Used as an identifier
Claim number: Used as an identifier
SSN: Used as an identifier
Benefit Type: Used for data records for accurate accounting and financial reporting
Payment/debt/collection amount: Used by VBA for to ensure accurate accounting and financial reporting
Payment/deb/collection date: Used by VBA to ensure accurate accounting and financial reporting

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The information created by the system will not be added to the individual's record. The functions performed are exclusively agency-specific accounting data analysis, reconciliation, and reporting. The analysis of the data is specifically analyzing the paper report or digital file format to correlate with expected locations of data elements. The input or report (e.g., .pdf, .csv, .docx, and .xlsx) is analyzed to determine how the data should be extracted from the source. The tool then extracts the data and subsequently transforms it (different unites, different aggregation units), to achieve the desired output.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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? (Ask ISSO)

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.

Immersion Cloud is an automated information processing tool that removes the time-consuming need to manually enter information for daily, monthly, and yearly reconciliation of financial accounts across the agency. The financial information is obtained and aggregated by OFM and loaded by VA system users into Immersion Cloud by the through a secure, browser-based file upload interface. The uploaded content may be of a variety of formats depending upon the system from which the information was obtained. This includes, but is not limited to, .pdf, .xlsx,

.csv, and .txt reports. PII processed and stored in the system is not collected from individuals. Instead, it is gathered from financial reports from agency systems in the OFM fulfillment of financial reporting under previously cited laws and regulations. Information produced by Immersion Cloud is used for agency financial controls and no information from Immersion Cloud is added to an individual's records.

All system operators and users are responsible for the protection of PII. Identification of PII is inherent in the operation of the system. The system user processes the data using a pre-built "model" (data capture, extraction, and transformation), tailored specifically to the input report content and format, as well as the desired output. Therefore, all system users are aware of the PII in the source material as well as the results. System operators are responsible for operating and monitoring system components. They have no need to access the PII although they have technical means. All actions of system operators, and associated system responses, are logged and reviewed per the System Security Plan and continuous monitoring efforts.

Immersion Cloud system users are managed by the VA System Owner and Contracting Officer Technical Representative (COTR). VA system users will be provided access as they on-board with the VBA OFM. When system users leave, whether they transfer elsewhere in VA or leave VA altogether, their access to Immersion Cloud is disabled by the VA System Owner. The VA System Owner conducts quarterly validations of the user repository to ensure those that do not need access have been disabled.

Potentially inappropriate access to, or handling of, PII is reported to the Immersion Cloud ISSO/ISSM who information the VA System Owner, who makes a report in accordance with VA organizational policies as well as VA Handbook 6500.2. VA may take disciplinary actions on contractor personnel independent of disciplinary action implemented by the contractor's employer.

Data processed by Immersion Cloud will be stored for ongoing reporting needs, it is expected that all system users would need access to the PII, if present. All data processed by the system is protected at rest and in motion by encryption techniques using a FIPS 140-2 validated security module. All privileged and un-privileged users are required to participate in agency-specified privacy and security training at least annually, and all individuals have passed suitability assessments appropriate for access to PII. Users are trained on the identification and mandatory reporting of all incidents that may have compromised the protection of PII.

The procedures and technical mechanisms used to protect private information are subject to continuous monitoring by system owners and operators in accordance with the System Security Plan and associated agency privacy controls. The system is assessed at least annually and during major modification for its ability to protect private information. System users are subject to the agency wide privacy monitoring and audit efforts.

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

The data retained in Immersion Cloud includes: Full Name, Social Security Number, Payment Amount, and Case (Claim) Number. The data is retained only to the extent that it will be aggregated or compared to different reporting periods. When no longer required, it is removed using the agency data retention policies and practices.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

The Immersion Cloud contract specifications require the ability to hold and protect all information for the duration of the contract. System operators will delete system data in accordance with the retention schedule specified by NARA. Per General Records Schedule (GRS) 1.1, Financial Management and Reporting Records, item #1, records will be destroyed when 3 years old, but longer retention is authorized if needed for business use: https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf. At the end of the contract, the operators of Immersion Cloud are required to return all customer data and remove the customer data with an approved information removal/obfuscation technique.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.

VA system owners and users are responsible for the removal of data. The retention schedule has been approved by the NARA. The guidance for retention of records is found in GRS 1.1 https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf and 3.1 https://www.archives.gov/files/records-mgmt/grs/grs03-1.pdf as approved by NARA: https://www.archives.gov/records-mgmt/grs.html

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

According to VA Handbook 6500, once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system, they are wiped clean and the data overwritten.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf

In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Immersion Cloud is not used for research purposes where research may involve PII. Any system-level testing and training is performed using simulated data.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

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 contained in the system will be retained for longer than is necessary to fulfill the VA mission

Mitigation:

1. System users only upload PII required for financial report aggregation.
2. To mitigate the risk posed by information retention, adhere to the NARA General Records Schedule and VA Handbook 6500. When the retention date is reached for a record, the individuals information is carefully disposed of by the determined method as described in VA Handbook 6500 (as outlined in section 3.4).
3. When an Immersion Cloud virtual server is taken out of service, the information is deleted and purged in accordance with the System Security Plan (SSP).
4. All VA users and Immersion Cloud security and operations team members must complete the VA Privacy and Security training according to agency requirements.
5. Data at rest is encrypted with a FIPS 140-2 validated encryption module.
6. Data transfer occurs using https encrypted with Transport Layer Security v1.2, FIPS 140-2 validated encryption module.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Financial Accounting System (FAS)	The IT system compiles and analyzes data from different places/formats and generates it into different aggregate reports.	First Name, Middle Name, Last Name, Payee, File Number (SSN), benefit type, payment/debt/collection amount, payment/debt/collection date	Text file, Comma-Separated Values (CSV), Microsoft Excel, Portable Document Format (PDF) Document Uploads
Benefit Delivery Network (BDN)	The IT system compiles and analyzes data from different places/formats and generates it into different aggregate reports.	First Name, Middle Name, Last Name, Payee, File Number (SSN), benefit type, payment/debt/collection amount, payment/debt/collection date	Text file, Comma-Separated Values (CSV), Microsoft Excel, Portable Document Format (PDF) Document Uploads
Financial Management System (FMS)	The IT system compiles and analyzes data from different places/formats and generates it into different aggregate reports.	First Name, Middle Name, Last Name, Payee, File Number (SSN), benefit type, payment/debt/collection amount, payment/debt/collection date	Text file, Comma-Separated Values (CSV), Microsoft Excel, Portable Document Format (PDF)

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
			Document Uploads

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

Follow the format below:
Privacy Risk: risk that the data could be shared with an inappropriate VA organization.

Mitigation: Consent for use of PII data is signaled by completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. Only personnel with a clear business purpose are allowed access to the system and information contained within. Review of access to all systems is done on a quarterly basis by the ISO and the security engineer. Clearance is required for each person accessing the system. Information is shared in accordance with VA Handbook 6500..

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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***
N/A				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Not applicable. This system does not share or receive data external of the VA boundary.

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: Although this system does not share information outside the VA boundary. Privacy information may be released to unauthorized individuals.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. This system adheres to all information security requirements instituted by the VBA Information is shared in accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring twofactor authentication.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

Veterans/beneficiaries provide the information voluntarily when they apply for Veteran Benefits, they continue to provide information to ensure the receipt of those benefits. This is not a source system and does not "collect" data, rather it uses reports from the source systems to provide further analytics required for financial reporting.

VA consistently publishes all SORNS to the Federal Register as dictated by law and VA Policy. VA requires the Administration and Staff Offices to put forth for approval and publication all notice for their respective Privacy Act system of records. VBA routinely updates SORN for altered system of record that include major changes or changes in the routine use. VBA ensuring that the required notice is given with requests for Social Security Numbers, and that a Privacy

Act statement appears on each applicable form or accompanying instruction sheet collecting information that is going into a Privacy Act system of records (see 5 USC 552a(e)(3)).

The applicable SORNs for this system are:

SORN notice 13VA047, Individuals Submitting Invoices Vouchers for Payment and Accounting Transactional Data
https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf

17VA26/78 FR 71727; Loan Guaranty Fee Personnel and Program Participant Records
https://www.govinfo.gov/content/pkg/FR-2019-04-17/pdf/2019-07647.pdf

36VA29/83 FR 44407; Veterans and Uniformed Services Personnel Programs of US Government Life Insurance
https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf

37VA27/79 FR 41744 Beneficiary Fiduciary Field Systems
https://www.govinfo.gov/content/pkg/FR-2014-07-17/pdf/2014-16810.pdf

38VA21; Veterans and Beneficiaries Identification Records Location Subsystem
https://www.oprm.va.gov/docs/sorn/SORN38VA21.PDF

58VA21/22/28 84 FR 4138; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records
https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

88VA244/83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CARS/CAROLS)
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

137VA005Q/74 FR 37309; Veterans Information Solutions (VIS)
https://www.govinfo.gov/content/pkg/FR-2009-07-28/pdf/E9-17910.pdf

138VA005Q/74 FR 37093; Veterans Affairs/Department of Defense Identity Repository (VADIR)
https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

VA 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records
http://www.gpo.gov/fdsys/pkg/FR-2014-01-23/pdf/2014-01286.pdf

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

No information is directly collected from the Veteran by this system so there is no opportunity to decline to provide information. A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to this system and other downstream applications.

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

All data for this system comes from others systems as noted in Section 1. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

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.

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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the source system.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

VBA provides individuals the right of access, under the Privacy Act, only to his or her records which are not exempt pursuant to subsections (j) and (k) of the Privacy Act. Access is given only to information which is retrieved by the individual's own personal identifier(s). Each VBA SORN as referenced in section 1.6 and 6.1 contains "Notification" and "Access" sections that indicate the official to whom such requests should be directed. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. VBA Privacy has submitted draft policy guidance to address the processing of Privacy Act requests. The policy draft is currently being reviewed by VBA Leadership.

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.

An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. Amendment requests must be in writing, signed, and must adequately describe the specific information the individual believes to be inaccurate (i.e., faulty or not conforming exactly to truth), incomplete (i.e., unfinished or lacking information needed), irrelevant (i.e., inappropriate or not pertaining to the purpose for which records were collected), or untimely (i.e., before the

proper time or prematurely) and the reason for this belief. Amendment requests can be mailed, faxed, or provided in person to the Privacy Officer at the facility where the Veteran records are maintained. VA does not allow an individual to verify identity by email.

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.

Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)." (4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. An approved VA notification of amendment form letter may be used for this purpose. (5) If it is determined not to grant all or any portion of the request to amend a record, the VA official will promptly notify the individual in writing.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend.

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.

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 a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: The information displayed in this system is obtained from other systems. If there is erroneous or inaccurate information, it needs to be addressed in those systems. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The team at VBA that will be using Immersion Cloud has a manual process of onboarding new employees to use their systems, and an equal process of offboarding/removing them from usage of systems. It is a manageable number of team members to monitor, and administrators receive

notifications of departure that trigger the offboarding process, ensuring that employees rolling off will no longer have access to the system. Additionally, a process of quarterly checks to ensure accurate accessibility is in place.

To obtain access to the source system reports, Applicants must request access via VA FORM 20-8824E or electronically using CSEM. A series of verification and approval levels are set up to ensure the applicant's information is valid and management approves of the access. Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and electronic signs he/she will abide by the VA Rules of Behavior. The user also must complete mandatory security and privacy awareness training. CSS Administrators and ISO have access to all CSS data. The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. The only authorized users (routine-user) are the System Administrator and the Information Security Officer. The SSN is used only for internal identification purposes. Usually it is the Information Security Officer who is first to notice a situation where the SSN or VA Claim Number in CSS does not match BIRLS or the access request form. ISOs have "read-only" access. Administrators cannot modify their own security record. In no situation is the end-user for which the security record was created would ever have access to their security record.

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 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.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractors are required to sign a confidentiality agreement as is required of the contractor onboarding process. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager

and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?
If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

FIPS 199 classification is Moderate. Target date for final operation is June 2021.

Section 9. 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.

Simon K. Caines 3430973

Digitally signed by Simon K. Caines 3430973
Date: 2021.04.15 11:47:55 -04'00'

Privacy Officer, Simon Caines

James M. McGee 926698

Digitally signed by James M. McGee 926698
Date: 2021.04.19 10:07:14 -07'00'

Information System Security Officer, Mark McGee

Yolonda J. Reese 220474

Digitally signed by Yolonda J. Reese 220474
Date: 2021.04.19 13:40:47 -04'00'

Information System Owner, Yolonda Reese

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).