U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Financial Business Management Systems (FBMS) - Tableau
Bureau/Office: Office of the Secretary
Date: June 14, 2019
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: 202-208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Financial Business Management System (FBMS) Tableau is a web-based publication and collaboration platform that allows authorized FBMS users to connect to share, view, and interact with data visualizations and data from the FBMS Business Warehouse (BW) and other data sources. Tableau provides user the ability to explore, interact, share, and analyze their data in order to make better fact/information based business decisions. The Tableau tool is used within FBMS to query relational databases, cubes, cloud databases, and spreadsheets to generate a number of graph types that can be combined into dashboards or images and shared over the Department of the Interior (DOI) network.

Any DOI bureau or office program can use Tableau to create visualizations. However, access and use is subject to the FBMS Reporting Tools Policy, DOI Acquisition Assistance and Asset Policy (DOI-AAAP-0142) and mandatory online Tableau for Publisher / Interactor Computer Based Training (CBT) training, and is strictly monitored for compliance with the policy. Users with the Publisher role can use data to create interactive workbooks on the desktop version of the software. These Analyses can be published to Tableau server to securely share non-sensitive data within the DOI bureaus and offices. Tableau allows for data to be sourced from other DOI systems external to FBMS. Examples of systems internal to DOI include: Incident Management Analysis and Reporting Systems (IMARS), Facility Management Software System (FMSS), and Safety Management Information System (SMIS).

FBMS Tableau is a minor application within the FBMS-Cloud boundary. All data sources are authorized for use within the FBMS-Cloud Tableau environment.

Tableau can also be used for sharing, distributing, and collaborating on content created in Tableau.

- **Shareable**. Tableau Publishers and Project Leads can create workbooks and views, dashboards, and data sources from data received from Tableau Interactors (user) on their Tableau Client, and then publish this content to the Tableau server. The folders are labeled with the bureau name "SHARE" which can be viewed by everyone who has an account and is assigned access to that folder. In accordance with FBMS Reporting Tools Policy, DOI Acquisition Assistance and Asset Policy (DOI-AAAP-0142), Tableau publishers and project leads (report developers) are responsible for validating that published visualizations and reports are reviewed for sensitive information and shared with the appropriate audience based on the sensitivity of the data.

- **Secure**. Tableau Server site and server administrators control who has access to server content to protect sensitive data from being uploaded in the visualizations. Administrators can set user permissions on projects, workbooks, views, and data

sources. All security rights are controlled by FBMS Security Personnel using the Server Administrative rights in Tableau servers.

Tableau allows DOI bureaus and offices to view, share, and create data visualization within FBMS Tableau Server. All data, analytics, and visualization contained within the Tableau are necessary for the support of DOI Business Process Operations, including, but not limited to, the following: support of the DOI's central accounting tasks, common processing routines and common data for many of the system's financial management functions, acquisition of goods and services, including tracking the status of requisitions, purchase orders, and contracts; recording and validating the receipt of goods and services; providing information needed to match invoices and issue payments; management of the DOI's travel and transportation activities; management of grants and subsidies to state and local governments, other organizations, or individuals; physical and accounting control over the Department's personal property; development and improvement of department owned land, buildings, structures, and facilities; and data collection and analysis for performance reporting.

C. What is the legal authority?

Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulations); 5 U.S.C. 5514, 5701 et seq.; 26 U.S.C. 6402; 31 U.S.C. 3511 and 3512, 3701, 3702, 3711; 40 U.S.C. 483; Public Law 106-107, and 41CFR 300-304; OMB Circular A-130, Managing Information as a Strategic Resource; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments", December 8, 2011; Presidential Memorandum, "Building a 21st Century Digital Government", May 23, 2012 and Departmental Regulations.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

FBMS Tableau is a Minor Application under the Financial Business Management System (FBMS) - Cloud UII Code - 010-000000316.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Other: *Specify the PII collected.*

Employee name, DOI Active Directory ID, government phone number, bureau are required to create a DOI FBMS Tableau account. FBMS Tableau users must be registered and approved to have an FBMS ID created to gain access Tableau. Once the FBMS ID is created users can access the Government Risk and Compliance (GRC) or Fiori via the FBMS Enterprise Portal and submit a GRC request for Tableau Interactor role or the users bureau lead or supervisor can submit the request for Tableau access. The bureau manager will then receive an email of the request and approve or disapprove the access request. Users will also need to complete the required online Tableau for Publisher / Interactor CBT training before access is granted. The CBT provides training to users based on their roles and requires the user's acknowledgment of understanding that PII or sensitive data may not entered or may not be used in Tableau visualizations.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Tableau uses GRC or Fiori to request, approve and apply security roles in the FBMS SAP environment. Users must submit GRC request to be granted Interactor role to access the Tableau application.

DOI records:
FBMS leverages DOI Active Directory group, role, and access authorization are specified according to Bureau and/or Office, duty descriptions and managers role recommendation.

Tableau uses DOI AD and DOI Personal Identity Verification (PIV) card for authentication. Users are then automatically federated to the Tableau. Tableau users must have a role assigned to them in the SAP Fiori and the GRC.

DOI bureaus and offices registered to use FBMS Tableau can upload their data into Tableau via flat files manually.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☐ Other: *Describe*

Website - Publicly available data on federal agency websites are collected and used for visualization purposes only by various bureaus and offices department-wide. Information can be collected from other data sources within the DOI manually can be uploaded into FBMS Tableau Client using any file type to develop a report that can be used for visualization in Tableau. Data is manually downloaded from internal or external data sources and are sent to the Tableau Publisher or Project Lead for review to ensure file

does not contain any PII. Only a formatted file type can be used as a source file to create visualization within Tableau. A text file cannot be used.

IMARS - Tableau data connection to IMARS server database is a secure connection. The DOI IMARS will only share statistical anonymous non-PII data and reporting metrics, such as number of Parks fire incidents with Tableau for data analytic and visualization purposes only. There is no PII and no risk of re-identification by Tableau users, only authorized officials in each bureau/office have access to the IMARS database.

Safety Management Information System (SMIS) - Tableau data connection to SMIS server database is a secure connection. SMIS will only share non-PII data with FBMS Tableau to create visualization for their users to view SMIS data analysis and reporting on safety risks, hazards and near misses in the workplace including on the job injuries. This data can only be viewed by SMIS users and will be reviewed by their designated SMIS Tableau Publisher to ensure no PII or sensitive data is published in the Tableau client "SHARE" folder for all users to view.

Facility Management Software System (FMSS) - Will use Tableau to provide visualization of their managed inventory assets and their assets conditions to include: Building, housing, campgrounds, water system, and paved roads. The data will only be accessible to FMSS users and all data uploaded will be non-sensitive and non PII.

The FBMS Tableau new Web Data connector (WDC) function allows for Bobj Webi to refresh and update the visualization in Tableau Client. Data must be in a table format to be exported using the WDC. Users use the Bobj and WEBi reports to update corresponding visualizations/visualization reports that have been published in Tableau client. Bobj and Webi Power users are responsible for not uploading sensitive or PII data. The Tableau Publishers still has the overall responsibility for reviewing the data before publishing in the Tableau Client.

Other DOI data sources external to FBMS is collected via an extract file. The FBMS Tableau currently does not allow any sensitive or PII data to be used in visualizations.

D. What is the intended use of the PII collected?

The FBMS Tableau Policy does not allow any sensitive or PII data to be used in visualizations. The publisher and project lead roles are responsible for checking all data for PII and sensitivity prior to being uploaded into Tableau in accordance with FBMS Reporting Policy, DOI-AAAP-O142 posted on the Tableau Client. PII is only used in the FBMS GRC and SAP Fiori to set up user accounts for access to Tableau. FBMS Tableau usernames are used for reporting the number of visualization created by a user within Tableau.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The FBMS Tableau does not allow any sensitive or PII data to be used in visualizations. FBMS Tableau Security team will have access to setup and manage security related tasks in Tableau including permissions, creating groups, setting up users and manage their access. FBMS Tableau Server site and Server Administrators control access to server content to protect sensitive data from being uploaded in the visualizations. Administrators can also set user permissions on projects, workbooks, views, and data sources.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

The FBMS Tableau Policy does not allow any sensitive or PII data to be used in visualizations. Each DOI Bureau, Office, data sources are setup in Tableau with their own folders. The folders are labeled with the bureau Name and "SHARE" which can be viewed by everyone who has an account and is assigned access to that folder.

Folders labeled with bureau name and "ONLY" only users with access to that folder can view executables labeled for that bureau or office only. No other bureau or office can access their folder without being granted additional access to the folder.

Publisher and Project lead role can view data within their bureau only and can do all edits including delete their bureaus information only. The Publisher can connect to or receive various data sources via email or to create visualizations to be published in Tableau. The Project Lead is overall responsible for the visualizations published within their bureaus project. The project lead can move content between projects, create and maintain Quality Access/Quality Control process required to publish to ensure best practices are maintained, and maintain an archive of deleted content for one year.

Guest access is available for use to share visualizations with users who do not have an account in Tableau. This access allows Tableau users to send a link to a visualization to someone to view. The link allows access to only that visualization and no other access to other Tableau visualization. The link is only accessible from within the FBMS boundaries. There is periodically review of data to ensure there is no sensitive or PII data in the reports. Each Bureau / Office Tableau Developer role follows a mandatory criteria for publishing a report for guest access prior to publishing a report for guest access published in the FBMS Reporting Policy, DOI-AAAP-O142 posted on the DOI Acquisition, Assistance, and Asset Policy (DOI-AAAP) Portal.

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Tableau Software Inc. provide system maintenance to FBMS-Cloud Tableau system, but have no access to data within the FBMS-Cloud system environment. Contractors who are assigned the Tableau Publisher or Project lead role will have the ability to design, develop, and publish visualizations in Tableau. Contractors can also be responsible for designing and developing the Tableau Application and maintaining the system.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Yes, users can decline to submit a Fiori for GRC request to set up their account to access Tableau. Employees are not compelled to provide their PII data, however all roles within Tableau must be identified in order to gain access to the system. Users can only be granted access to Tableau via Fiori or GRC request.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA.

Users must log into the DOI network with their PIV card to access Tableau through the FBMS Enterprise portal. Employees must agree to being monitored in accordance to DOI policy for security and other authorized purposes prior to accessing the FBMS Enterprise portal. Also, a link to DOI's Privacy Policy is located at the bottom of the FBMS Enterprise portal landing page.

FBMS-Cloud users are presented with the following Terms and Conditions of Use prior to signing on to the DOI network or application: Terms and Conditions of Use

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

☒ Other: *Describe each applicable format.*

FBMS Tableau users must also read and agree to the OS- BIO-6024-SE-005 Tableau Privacy Policy before accessing the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

This system does not retrieve PII. The Tableau Publisher or Project Lead role has the rights to retrieve the data in the Tableau Client. Data can be retrieved via file type and name; database file, excel file report or the data can be developed into a visualization and then be retrieved and downloaded from the Tableau website located on the FBMS Portal in an image, portable document format (pdf), or workbook form. Tableau Interactors can not download data, they can only download the visualization in a .pdf, image file or a cross tab version of the data being used in the visualization.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*
☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The Project Lead and Publisher for each bureau or office can receive and upload data into Tableau. No other role can upload data into Tableau to create visualizations. Both publisher and project lead is responsible for checking all data for sensitivity and accuracy prior to being uploaded into Tableau in accordance with FBMS Reporting Policy, DOI-AAAP-O142 posted on the DOI Acquisition, Assistance, and Asset Policy (DOI-AAAP) Portal. Non-conforming data will be posted to a suspense file for additional examination and resubmission upon correction.

B. How will data be checked for completeness?

The visualization creator and the Tableau Publisher will check the data for completeness prior to being uploaded and entered into the Tableau. The Publisher and Project Lead role is responsible for determining if the data is complete and checks data for sensitive information.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The data owner will determine if the data needs to be refreshed to update the visualizations. This could be done daily, weekly or monthly, depending on the report and the data owner and the type of data that needs to be refreshed.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Tableau is located in the FBMS-Cloud boundary, which follows the same retention period as the FBMS data. Retention periods for FBMS vary as records in FBMS are maintained by subject matter in accordance with the applicable Department-wide, bureau or office records schedule, or General Records Schedule, approved by the National Archives and Records Administration (NARA) for each specific type of record maintained by the Department. Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor.

The FBMS Tableau data is maintained under Department-wide Records Schedules (DRS), DAA-0048-2013-0001, which was approved by NARA.

Data, analytics, and visualization records in FBMS Tableau in support of DOI Business Process Operations, will be maintained under 1.3B Long-term Financial and Acquisition Management. Records are temporary and are cut off as instructed in the bureau manual

or at the end of the fiscal year in which the files are closed, then destroyed 7 years after cutoff depending on the record.

Tableau system information and user data will be maintained under 1.4, Information Technology, System Maintenance and Use records. These records are temporary and cut off as instructed, then destroyed 3 years after superseded or obsolete.

Bureaus, offices, programs and data owners are responsible for managing their own records for visualizations created and maintained in Tableau in accordance with the specific records retention schedules for the subject matter of the record or visualization created for their organization.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Currently FBMS Tableau retains all records while FBMS is implementing an Information Lifecycle Management (ILM) Tool in 2019, which is expected to be fully deployed in 2020 to manage records and data in the system. Tableau data and visualizations will be disposed of in accordance with the applicable record schedule and Departmental policy. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Privacy risks within the FPPS boundary are related to data being uploaded and maintained from systems external to the FMBS boundary for reporting and visualizations that may contain sensitive information. In an effort to mitigate this risk, all data sources external to the FBMS boundary must be registered, reviewed and approved for use in a report or visualization. The GRC external data registration request requires approval from a Bureau designated Data Representative and FBMS ISSO. The registration requestors are notified of approval or rejection decision via email and stored in GRC. All data for visualizations or reports in Tableau are reviewed for appropriate inclusion in the FBMS reporting environment. In addition, Risk Acceptance (RA) will be required before the data can be uploaded in Tableau. Once the RA is approved by the authorizing official of the data source system and Tableau, the DOI internal data sources will be authorized for use. The Tableau Publisher is responsible for reviewing all data prior to the data being uploaded in the Tableau.

There is a risk that data is shared from DOI systems with sensitive PII, Privacy Act systems, or systems categorized as High impact level such as IMARS. The FBMS Tableau does not allow any sensitive or PII data to be used in visualizations. Privacy risks are mitigated through a series of administrative, technical and physical controls.

Tableau Publishers, and Project Leads are required to complete and acknowledge the Tableau for Publisher CBT, DOI Role-Based Security Training (RBST), DOI Role-Based Privacy Training (RBPT), and sign the Tableau Memorandum of Understanding (MOU) before access is granted. Tableau Interactors are required to complete Tableau for Interactors CBT, acknowledge their understanding not to publish PII data to the Tableau Server. Only data categorized as FISMA Low or Moderate and appropriate will be used in Tableau for visualization purposes. All access to this visualization or report is controlled by authentication methods to validate the approved user. The Tableau Publisher is also responsible for viewing all data for sensitive data prior to uploading visualizations in Tableau.

To mitigate the risk of exposure of sensitive data from IMARS, responsible officials acknowledged in the Tableau for Publish CBT that only non-PII statistical data (anonymized and aggregated for program management and metrics) at the low or moderate level in Tableau from a siloed non-PII IMARS database that complies with all requirements of the FBMS Reporting Policy, DOI-AAAP-O142 posted on the DOI Acquisition, Assistance, and Asset Policy (DOI-AAAP) Portal. Only authorized DOI law enforcement users will have access to view these metrics in visualizations in FBMS Tableau system. Only DOI IMARS data categorized as FISMA Low or Moderate and appropriate will be used in Tableau for visualization purposes. All access to this visualization or report is controlled by authentication methods to validate the approved user. The IMARS Tableau Publisher is also responsible for viewing all data for sensitive data prior to uploading visualizations in Tableau.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. An audit trail of activity will be maintained sufficient to reconstruct security relevant events. The BIO follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. Tableau Publishers, and Project Leads are required to complete and acknowledge the Tableau for Publisher CBT, DOI Role-Based Security Training (RBST), DOI Role-Based Privacy Training (RBPT), and sign the Tableau Memorandum of Understanding (MOU) before access can be granted. Tableau Interactors are required to complete Tableau for Interactors CBT, acknowledge not publish PII data to the Tableau Server.

There is a risk that individuals may gain unauthorized access to the information in the system. All access is controlled by authentication methods to validate the authorized user. Access to the DOI network requires two-factor authentication which single sign-on (SSO) is enabled to allow users to access Tableau via the FBMS Portal. Risk is mitigated by limiting access and publishing rights to only the Project Lead and Publisher roles. Users are granted authorized access to perform their official duties and must comply with the principles of separation of duties. User group, role, and access authorization are specified according to Bureau and/or Office, duty descriptions and managers role recommendation, which requires their DOI Active Directory credentials for system login

using their PIV card before access can be granted to the FBMS Information System. Safeguards for information security and privacy are compliant with and maintained in accordance with OMB A-123, Management's Responsibility for Internal Control, and NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. DOI users of FBMS are required to complete the DOI mandated annual Federal Information Systems Security Awareness (FISSA), privacy awareness, and records management training, and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Data maintained in FBMS Tableau is protected by FIPS 140-2 compliant Data at Rest encryption at the database level.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Data in Tableau does not contain PII or sensitive data. Records retention schedules falls under DOI FBMS system boundary retention schedule, IT records schedules and bureau/office program specific records schedules. Currently FBMS Tableau retains all records. FBMS is implementing an Information Lifecycle Management (ILM) Tool in 2019, which is expected to be fully deployed in 2020 to manage and dispose of records and data in the system. Tableau data and visualizations will be disposed of in accordance with the applicable record schedule and Departmental policy.

FBMS Tableau is a minor application under the FBMS-Cloud Information System. The FBMS-Cloud system has undergone a formal assessment and authorization in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. FBMS Tableau is a cloud system rated as FISMA moderate based upon the type of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the data contained in the system. A security plan was completed to address security controls and safeguards for the FBMS Tableau system. The use of DOI IT systems is conducted in accordance with the appropriate DOI acceptable use policy. Additionally, all system interconnections are authorized by the respective system Authorizing Officials (AO) and the security controls for the interconnection will be documented in the Interface Design Specification document and referenced in the Tableau System Security Plan (SSP).

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

Tableau is a minor application located in FBMS-Cloud boundary which FBMS is an enterprise-wide financial management system that consolidates the majority of DOI's business and financial management functions.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

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

Not Applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users

☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

Tableau Interactors with the proper security role in Tableau will have access to their data but is limited to what can be done with the data. The Tableau Publisher and Project Lead roles will have access to the data and have the right to edit, delete, modify, and publish the data within the Tableau Client. The Publisher role can only upload extracted files to input their data in the Tableau Client and will only have access to the data in their folder. FBMS Developers customize the Tableau application.

FBMS Tableau system administrators and contractors perform system maintenance, manage server configuration, create sites and projects, and other related activities, may have access to the data in the Tableau server.

Users who have "Guest" type user access in Tableau will be able to access non-sensitive reporting data via the visualization distributed through the reporting link. The link does not allow the guest user to navigate to other visualization in any of the other Bureau shared folders. The link can be shared with users with no Tableau account.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Bureau/Office administrators are responsible for controlling and monitoring access of authorized employees. Bureau/Office Administrators and authorized employees will only receive access to data for their own Bureau or Office unless performing the role of a cross-servicing user. A user must have a valid DOI UAM account prior to being able to submit a new role request in GRC. The request is initiated in GRC and processed through automated approvals by the requisite parties (Bureau Security Points of Contact (SPOCs) and Bureau Account Controllers). The SPOC and Account Controller must approve the new user registration request before the user is granted access to FBMS. Role requests are also initiated in Fiori or GRC and processed through automated approvals involving Bureau Security Points of Contact (SPOCs), Bureau Account Controllers, Bureau Internal Controls Coordinators, and Bureau Training Coordinators.

Tableau interactors (users) are restricted from accessing any backend data in the Tableau client or on the server. The only data Tableau interactors can view is data that is published in the visualization or the report in a folder for which the users have expressly granted permissions.

Tableau follows the FBMS Governmental and Departmental standards for application access controls. Tableau Publisher and Project Lead who have created a visualization to be published have access to only their data used to create the visualization. The Publisher

and Project Lead is the final authority for publishing the data in the Tableau client. All Tableau data is stored on the Tableau server and only authorized Tableau Publisher and Project Leads can access the data.

Users who have "Guest" type user access in Tableau will be able to access non-sensitive reporting data via the visualization distributed reporting link only.

These users access controls apply to all data hosted on the Tableau server including data from the DOI internal and external data sources.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors who are assigned the Tableau Publisher or Project lead role will have the ability to design, develop, and publish visualizations in Tableau. Contractors can also be responsible for designing and developing the Tableau Application and maintaining the system. Privacy Act contract clauses are included in all contractor agreements.

BIO contractors are required to sign non-disclosure agreements as a contingent part of their employment and are also required to sign the DOI's Rules of Behavior and complete FISSA and privacy training prior to accessing a DOI computer system or network.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

Tableau audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system, to include attempts to access files, analytics or visualizations beyond the user's assigned permissions or role. The logs capture account creation, modification, disabling, and termination in the logs. The application name, date and time is captured, item ID, type, location, event type date and action taken on item is captured in the logs. Audit logs are enabled on all host and server systems as well as firewalls and other network perimeter security devices and Intrusion

Detection Systems (IDS). All logs are stored on the Tableau server and are automatically rolled up to the Security Information and Event Management System (SIEM) for consolidation, analysis, retention, and reporting purposes.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Audit settings are enabled in the FBMS-Cloud system boundary include directory service access, successful or unsuccessful logon events including the logon ID, date and time of each log-on attempt, and date and time of each logoff, object access, privilege use, system events, account management, devices used, and functions performed while logged on. These events are sent to and monitored by DOI OCIO.

Tableau audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system, to include attempts to access files, analytics or visualizations beyond the user's assigned permissions or role. The logs capture account creation, modification, disabling, and termination in the logs. The application name, date and time is captured, item ID, type, location, event type date and action taken on item is captured in the logs. Audit logs are enabled on all host and server systems as well as firewalls and other network perimeter security devices and IDS.

All logs automatically roll up for consolidation, analysis, retention, and reporting purposes. The system is also configured to automatically email the FBMS Basis and FBMS Information Assurance (IA) team for any Moderate severity events from the FBMS boundary.

M. What controls will be used to prevent unauthorized monitoring?

Only the FBMS Tableau system administrators can monitor users activity and the system administrator role is assigned only to a limited group of subject matter experts. Access to the system administrator role is assigned through the GRC system and requires proper authorization.

Controls outlined in the FBMS Tableau System Security Plan adhere to the standards outlined in NIST SP 800-53, Revision 4, Recommended Security and Privacy Controls for Federal Information Systems, are in place to prevent unauthorized monitoring. This includes the use of role-based security training, encryption, and maintaining data in secured facilities, among others. FBMS assigns roles based on the principle of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any FBMS assets.

FBMS IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Only authorized users with valid DOI Active Directory credentials will be able to access the system. In addition, all users must consent to DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training, and Privacy Awareness Training before being granted access to the DOI network or any DOI system, and annually thereafter.

FBMS-Cloud has Single Sign-On (SSO) enabled, users who log onto the DOI network can access the Privacy Policy via the link located at the bottom of the FBMS, Enterprise Portal page or the DOI.GOV website. Users must use PIV card and can only access FBMS-Cloud within the DOI network.

FBMS-Cloud users are presented with the following Terms and Conditions of Use prior to signing on to the DOI network or application: Terms and Conditions of Use

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards

☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

1. Transport Layer Security (TLS) 1.2 Enabled
2. Role Based Access Control (RBAC)

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

The FBMS Tableau currently does not allow any sensitive or PII data to be used in visualizations. Tableau Publishers, and Project Leads are required to complete the Tableau for Publisher CBT and DOI RBST, RBPT, and sign the Tableau

Memorandum of Understanding (MOU) before access can be granted. Tableau Interactors are required to complete Tableau for Interactors CBT.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director, Office of Financial Management serves as the FBMS Tableau Information System Owner and the official responsible for oversight and management of the FBMS security and privacy controls and the protection of information processed and stored by the FBMS Tableau system. The Information System Owner, Information System Security Officer, and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in FBMS Tableau.

The DOI Publisher and Project Lead roles within each Bureau / Office are responsible for reviewing the data prior to publishing in FBMS Tableau. Data owners are responsible for their own records and responsible for protecting the privacy rights of individuals for the information they use in the FBMS Tableau system.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The FBMS Tableau Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The FBMS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures.

Each DOI Bureau / Office is responsible for the management of their own data and visualizations, and reporting any potential loss, compromise, unauthorized access or disclosure of data resulting from their management of the data in accordance with DOI and Federal policy.