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: Bison Support System (BSS)
Bureau/Office: Office of the Chief Information Officer
Date: August 3, 2022
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?

Bison Support System (BSS) is a software and web-based IT Service Management application system (ITSM) deployed by the Department of the Interior (DOI) to provide a framework for storing, accessing, and managing DOI incidents, changes, and work orders using consistent processes. BSS will support the lines of businesses bureaus and offices, including business, financial, and IT services. BSS processes customer requests for bureaus and offices and supports the Federal agency customers. BSS also supports the DOI Cyber Incident Response Center (DOI-CIRC) and DOI enterprise-wide security incident reporting activities.

The DOI Office of the Chief Information Officer (OCIO) is responsible for managing and maintaining the BSS. The Customer Support Center (CSC), Service Delivery Division within the OCIO uses BSS to capture and process all change requests, incidents and problem reports. BSS also provides support to the lines of business applications for incident management, Change Management for managing infrastructure changes, Asset Management for data center inventory tracking and infrastructure management, and the Service Request Management. BSS enables DOI to automate and process customer needs to improve business processes and optimize the deployment of solutions and resources. BSS is hosted in the OCIO Data Center Boundary and consists of the following modules:

- **Incident and Problem Management** - Ticketing system for reporting, tracking and resolving customer issues and requests for supported applications, products and services, including DOI cyber security incident tracking service.
- **Work Order Management** - Automated work assignment for processing customer requests.
- **Asset Configuration Management** - Manages IT assets to support system management. Assets include items such as servers, network devices, storage solutions, software, etc.
- **Change and Release Management -** Manages changes in the IT hosting environment and the IT infrastructure (e.g., host, network or databases).
- **Work Order Management** – Manages data collection web interface for users to enter service requests into the BSS.
- **Service Level Management** - Measures service levels within the system for response and closure of incidents.
- **Knowledge Management** - Access point that contains BSS resources and allows users to search the BSS database for incidents, guides, or work instructions.
- **Discovery Tool** - Scans DOI network and collects information needed for asset management.
- **SmartIT** – SmartIT provides a graphical user interface to BSS applications.
- **Digital Workplace (DWP)** - BMC Software (BMC) Digital Workplace is a self-service application for business users to connect with IT and Human Resources (HR) at any location or time or on any device.

    - **BMC Remedy Classic:** Legacy IT Service Management consoles for request, work order, incident, change, task, problem and asset that will primarily be used by BSS administrators. May occasionally be used by BSS support users as needed.
    - **Control-Management:** Programmatic interfaces that provide developers and engineers ability to schedule, manage, and monitor defined workflows. Workflows can be integrated with other BMC BSS applications.
    - **Client Management:** An advanced systems management software that provides a reliable way to monitor all systems on a network. Provides an accurate view of

software installations, ensures device adherence to organizational and industry policies, and supports systems and software currency.

- **Truesight:** Delivers end-to-end performance monitoring and event management. It uses Artificial Intelligence for IT Operations (AIOps) to dynamically learn behavior, correlate, analyze, and prioritize event data so IT operations teams can predict, find, and fix issues faster.

This is the initial Privacy Impact Assessment (PIA) for BSS and will be updated as the system is implemented to reflect any changes or processes and to address any identified privacy risks as bureaus and offices begin using the BSS system.

C. What is the legal authority?

Departmental Regulations, 5 U.S.C. 301; 44 U.S.C. §§ 3551-3558, Federal Information Security Modernization Act (FISMA) of 2014; E-Government Act of 2002; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, "Managing Information as a Strategic Resource" July 16, 2016; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service", April 11, 2011; 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; Presidential Policy Directive (PPD)-41, United States Cyber Incident Coordination, July 26, 2016; National Institutes of Standards and Technology (NIST) Special publication 800-61, Computer Security Incident Handling guide; and US-CERT Federal Incident Notification Guidelines.

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*

UII Code: 010-000002539. The BSS System Security and Privacy Plan is under development.

☐ 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	N/A	N/A	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

BSS is not a Privacy Act system of records. It is a customer service and help desk ticketing system. However, it is an internal system which will support numerous DOI HR, financial and other systems including: DOI Lumen Enterprise Service Network (ESN), DOI Federal Personnel and Payroll System (FPPS), FPPS Datamart, DOI Talent, eStaffing, Entrance On Duty System (EODS), Quicktime, TMS/FedTalent, WebTA, Workforce Transformation and Tracking System (WTTS), E2Solutions, FM Travel (Concur Government Edition (CGE)), Financial and Business Management System (FBMS), Travel-CGE, Oracle Federal Financial (OFF), Technical Innovation and Professional Services (TIPS), Incident Management Analysis and Reporting System (IMARS), eLMS and the DOI-CIRC security incident reporting portal. The DOI records in the supported systems of records are maintained by the DOI system managers under government-wide, DOI, and bureau or office system of records notices (SORNs), and SORNs published by external agency customers who own the data that is being processed by DOI under a servicing agreement. DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn.

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

☒ Yes: *Describe*

Per the Information Collection Clearance Officer (ICCO) and Departmental Forms Manager, this information collection does not trigger the Paper Reduction Act (PRA) because they are internal, and the information is collected from Federal government employees or contractors acting within their duties or customers who are supported by bureau or office programs. The program officials will work with the ICCO to review the forms to determine if there are PRA requirements for external customers.

System request forms generated by the DOI bureau/office customers are owned and managed by bureaus/offices and program offices who are responsible for ensuring the forms are authorized to be used. BSS administrators developing a request form shall ensure only required non-sensitive PII information is being requested from the customer.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Employment Information – active or inactive status
☒ Military Status/Service – active or inactive status
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

The BSS self-service portal will provide IT Helpdesk support services to DOI bureaus and offices. PII that will be collected and maintained in the system includes DOI employee cell phone number, work email address, and desk/office phone number. BSS does not request or store any SSN or sensitive PII related information within its boundary.

Customers may provide personal contact information, such as email address and phone number, for the CSC to communicate with current and former employees when a business need requires it.

BSS supports numerous agency customers and the PII types vary by customer and line of business. Customer data in BSS is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act. BSS CSC staff access customer data to provide support to each customer and only have limited access as determined by the customer agency.

For example, BSS provides technical support to the Bureau of Indian Education (BIE) education Learning Management System (eLMS), which is a centralized system for students, teachers, parent/guardians, administrators, Education Resource Center (ERC) staff, and the Central Office staff. Data will be synchronized from the BIE Azure Active Directory (AD) system to create, authenticate, and manage user accounts for educational staff and students. PII will include first name, last name, school, organization, official school email address, official school phone number, and school location address. The customer may provide more information in order to assist in resolving a ticket.

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*

PII may be collected from contractors, volunteers, and vendors. Some PII information is collected from the various security tools used for cybersecurity reporting and security incident investigation. This data is maintained in the DOI-CIRC portal and other security monitoring systems, and is not stored in BSS. Please refer to the DOI Bison Shield PIA for more information.

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 *Describe*

BSS supports customers through the DWP portal to create helpdesk tickets and view the status of the tickets submitted. Users may have access to view the BSS ticket information for their bureau/office. There is no interface connections between BSS and other systems/applications that BSS supports. BSS CSC Tier 1 service personnel would access the systems that BSS to manually pull data for the purposes of data validation, they would not change or store the data as requested for an authorized purpose.

DOI internal user profile information is initially set up through DOI Active Directory service (AD). BSS syncs with Azure AD for eLMS users and DOI AD for other DOI users to create customer accounts, identify, and authenticate users to the system. Users without a PIV card will be provided with user credentials in order to login to BSS. BSS People Profiles are synchronized with DOI AD using the Lightweight Directory Access Protocol (LDAP) over secure socket layer. The query used against AD searches the Global Catalog (across domains) for enabled user accounts that have an email address associated with it. The query filters out elevated privilege accounts, contact records, and service accounts.

☒ Other: *Describe*

The customer contact information is collected and entered into BSS which will be referred to the appropriate office for action when the customer submits requests to the CSC Help Desk. The customers can call, or email, or fax to report issues to the help desk, or they can submit requests through the DWP.

Fax, Email and attachment:
The CSC works with the customer to resolve the issue and is responsible for updating and closing the ticket, documenting any actions taken, and providing a description of the resolution. One of the features that assists support staff with the tickets is an email integration capability within the incident management application that automatically converts incoming emails including documents attached in the customer's email to incident requests. In addition, the CSC will review the tickets/requests and forms/attachments submitted by the automated email system for PII data. A user fills out a form to be submitted to the CSC, which may require supervisor authorization. If the form or email contains PII data then the PII data will be removed from the BSS system. Forms with PII are faxed to the CSC.

Website:
Information may also be provided through the DWP, which provides an online user self-service interface from which employees can view and request services that are available to them. This is one of the self-service automated processes that was developed to assist the customers with requesting services without having to go directly to the Help Desk. Information is manually retrieved/verified by help desk staff from the systems that BSS supports to research and document the customer request. Help Desk personnel have read access to many systems supported by the CSC to assist the customers with their requests. In some limited cases, the Help Desk personnel have write access to designated applications. For the remaining customer access to systems, the Help Desk uses Bomgar to remote into machines.

Phone call:
Any user can call the help desk to open a ticket to request various services, such as IT system access, application requests, travel, etc. The CSC may need to create a customer profile record for users who are not in the system to create and process the service ticket.

Information sharing within BSS:
The BSS modules use the same database and can access the table of data relevant to the operation of a specific module. This is a critical and necessary aspect to providing full IT Service Management capability. Users are assigned roles in the system and these are assigned by the BSS module the user may need access to. The users are always given the least privilege necessary for the user to perform their job function. For example, a customer calls into the CSC with a laptop issue. The laptop is stored in the BSS Asset Configuration Management module and can be linked to the incident and associated to the customer so all data is aggregated together for the customer. Another example could be that multiple people are affected by the same issue so multiple incidents get created, such as for a network outage. Because of the impact and the urgency associated with this the IT team decides that a problem needs to be created and associated to these incidents so that a root cause and solution can be identified to resolve the issue. Once the problem root cause and solution have been identified a change request is necessary in order to implement the permanent fix. It is essential that these specifically identified limited dataset be shared between these modules.

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

PII will be used create user accounts, authenticate, and grant users access to the BSS ticketing system to document and process customer requests. The BSS IT Helpdesk support staff will use PII data to contact users about their incident tickets. Tickets created may include some PII information which are routed for resolution purposes to the Tier 2 administrators of the supported applications where the PII are originally maintained.

The CSC does not allow PII related forms to be uploaded as an attachment in BSS. Standard procedures have been developed in order to process forms and are no longer tracked and/or processed in BSS. Forms that are submitted to the Helpdesk are not processed in BSS and will be forwarded to the appropriate POC for processing. Some sensitive PII may be found in attachments when users choose to provide or upload information so as to update their PII information in the systems that BSS support. Sensitive PII is not requested or required from the BIE user to access BSS or to receive IT Helpdesk support services.

The DOI-CIRC incident tracking function in BSS is specifically designed with data privacy protection mechanism which does not allow attachments to be uploaded into BSS. Attachments may be loaded from the custom forms, but a warning exists for the limited number of support personnel who have access to this form not to upload information containing PII.

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.*

PII provided by DOI agency customers are shared within the OCIO to process and resolve customer issues and requests and for tracking DOI cybersecurity incidents reported. Forms containing PII are faxed to the CSC within the OCIO. The CSC faxes these forms to the appropriate Tier 2 group for processing.

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

Only limited PII may be shared with other bureaus/offices as needed to resolve tickets. Users from each bureau/office are only entitled to view tickets associated with their bureau/office.

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

Some specific PII of the employees of other Federal agencies can be shared with Federal agency customers to resolve their employees' specific requests. This data is not stored in BSS. Reports are only shared upon request from the Federal agency customer. The data collected for cybersecurity incident tracking purposes might be shared with those corresponding authorized personnel in other Federal agencies, such as Department of Homeland Security (DHS) US-

CERT, as well as local and Federal law enforcement agencies on a “need-to-know” basis connected to the specific incident being processed.

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

Some specific PII can be shared with Tribal, or State agency customers to resolve their specific incident requests. Reports are only shared upon request from the Tribal, or State agency customers.

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

DOI contractor staff who provide support for the BSS system and its customers have authorized access to BSS system and data which are the subject of the issues in order to perform their duties.

The contractor personnel assigned to the DOI-CIRC, DOI threat, and DOI enterprise messaging teams with a need to know directly connected to the specific incident reported may have access to the data of the specific incident processed by BSS support service.

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

The enhancement or replacement of DOI network devices or equipment necessitate the change management processes of BSS. DOI vendors are authorized as DOI network users to access BSS via DOIApps and will have a PIV card and authenticated on the DOI Network to complete the specific task through a DOI work order. Government Furnished Equipment (GFE) will be required for this access unless a waiver is granted from security for the vendor to be allowed to use personal equipment.

Once the vendor is in the BSS system they will be isolated to only the data they are allowed to see and manipulate within the system. They will be working assigned tasks in the Incident and Problem Management module to conduct a technical analysis for circuit order requests.

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.*

All requests for BSS support are inbound requests to the CSC/IBC/OCIO. Individuals will need to submit their contact information to process requests as appropriate. Submission is voluntary, however, failure to submit requested information may result in delay of resolution of issues.

During the service process, the BSS system might process incident information of its supported systems, including cyber security incident management and tracking tools. The privacy risks of these tools are assessed separately in the DOI Bison Shield PIA.

☐ 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.*

BSS collects information from individuals on behalf of agency customers. Forms generated by the DOI bureau/office customers, such as payroll forms, HR, and traveler profile forms with PII information, are owned and managed by bureaus/offices and program offices who are responsible for ensuring the forms are authorized to be used and that Privacy Act Statements are included in the approved forms that collect PII for applicable Privacy Act systems.

☒ Privacy Notice: *Describe each applicable format.*

Notice is also be provided to individuals through this PIA and any related PIAs and SORNs for systems that are supported by BSS.

A Privacy Notice is placed at the BSS URL login and collection sites where individual employee customers submit requests for assistance. DOI Privacy guidelines are provided where the DOI clients can retrieve for reference.

☒ Other: *Describe each applicable format.*

CSC employees may attach documents and enter work information for Tier 1 and Tier 2 customer requests. A statement will be placed next to the “Attach” or “Upload” button to inform CSC employees not to upload documents that contain sensitive PII into BSS.

☐ None

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

Information is retrieved manually by individuals who are authorized to access the system using incident ticket number, customer name, customer email, reports generated by BSS help desk and system support users or automatically for customers, and tickets assigned to the Tier 1 and Tier 2 application support users or groups. Cybersecurity incident tracking can be retrieved by incident number, ticket number, ticket type, name of Point of Contact (POC), date of incident or by doing a keyword search on any field within the database. The only way to query by name is for queries involving name of the creator of a ticket or the assigned POC of a ticket. The association of these names to incidents is in relation to their official government duties.

A user submits a request through the DWP self-service portal. The CSC or bureau/office Help Desk will review the tickets/requests and forms/attachments submitted for PII data. If the request contains sensitive PII data, then the PII data will be removed from the BSS and the form will be processed externally through fax. Request forms that are no longer used will be taken offline so they are no longer available for use. Requests the Helpdesk are unable to resolve will be forwarded to the appropriate BSS IT Help Desk group for processing.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports can be created and distributed for the purpose of workload reporting, volume reporting, and projections. Users can pull a report on the history of incident tickets created in the BSS portal. Reports are only shared upon request from the Federal agency customer. There is no PII data in the reports. The reports are reviewed and any PII are scrubbed before sharing.

☐ No

Section 3. Attributes of System Data

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

BSS provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the BSS system might trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information to properly address the inquiry and troubleshoot the payroll, HR or other customers issues and requests.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

B. How will data be checked for completeness?

BSS provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the BSS system would generally trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information to properly address the inquiry and troubleshoot the payroll, HR or other customers issues and requests properly. In addition, the BSS Tier 1 and Tier 2 support staff ensures the incident and change request ticket is complete and all required information is entered or attached to resolve or escalate the customer request.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

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

BSS provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the BSS system would generally trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information so as to address the inquiry and troubleshoot the payroll, HR or other customer's issues and requests properly. Data in BSS, including attachments, may be manually verified with the systems/applications that the BSS supports to ensure data is current, as needed, to resolve or escalate the customer request.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

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

Official records maintained in the BSS system are held in accordance with DOI's Administrative Departmental Records Schedule. Records of Business Services (for ordering property) are covered in Section 1, Short-term Administration Records (DAA-0048-2013-0001-0001). All others fall under Section 4, IT Information. Three areas within that section separate the records with retentions between 3 and 7 years. The sections are System Maintenance and Use (DAA-0048-2013-0001-0013); and System Planning, Design, and Documentation (DAA-0048-213-0001-0014); and Long-term Information Technology Records (DAA-0048-2013-0001-0015).

Records processed on behalf of customers are maintained in customer systems and are covered under their applicable records retention schedules.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

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.

There are moderate privacy risks for use of the BSS system due to the nature and volume of PII used to provide support to customers. DOI uses a series of administrative, technical and physical measures to ensure that adequate security and privacy controls are selected and put into place to mitigate these risks. BSS provides the framework for storing, accessing, and managing DOI incidents, problems, work orders, IT changes as well as asset inventory and supports many systems for DOI, including those that provide shared service to federal agencies customers through the incident and change management processes. DOI will also use BSS to record and track cybersecurity incidents using the DOI-CIRC process. The PII provided by the users of the BSS system as the subject of the incidents or the POC information provided by users for follow-up of issue resolution are an inevitable part of the data that BSS handles.

Even though the systems that BSS support do not directly transfer PII into the BSS system, there is a risk that the PII may be inadvertently entered into the BSS system in the process of creating an incident ticket, which are removed when detected. DOI mitigates this risk with a statement that instructs users not to enter or attach any files that might contain PII information not required for creating an incident ticket.

There is a risk of inadequate notice to individuals. Notice is provided to users through the publication of this PIA, any related PIAs and SORNs for systems that are supported by BSS, and the BSS Privacy Notice posted on the entrance page within the system and DOI Rules of Behavior (ROB). The BSS tickets might reference records containing PII, however, BSS does not collect nor process PII other than what the customers/data subjects already consented to provide to the government or to federal agency employers to fulfill their official duties. The PII is originally collected via proper notice and consent processes, such as through the published PIAs and DOI-wide or government-wide SORNs, obtaining OMB approved form control numbers, and providing Privacy Act Statements on forms.

To mitigate the risk of unauthorized disclosure or misuse of the PII or use for an unauthorized purpose, the CSC team has an established process that sanitizes the work reports CSC generates so as to ensure the reports will not contain PII. Data sharing is strictly for the purpose of issue resolution or incident tracking and for purposes as identified in this PIA. The customer data, including PII, will not be used for any other purposes, and will not be repurposed under any circumstances. DOI requires its employees and contractors to complete security and privacy awareness training during the on-boarding process. All DOI employees and contractors are required to complete annual Information Management and Technology (IMT) Awareness training, which includes cybersecurity, privacy, records management, Paperwork Reduction Act, Controlled Unclassified Information, and Section 508. Individuals accessing the BSS system also complete annual role-based privacy and security training. Training completion is tracked and monitored in DOI Talent, the Department's learning management system. The DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI ROB.

CSC pre-defines specific datasets used for this specific purpose and synchronizes it with the BMC discovery tool which stores agency protected information such as server name, IP address, server location, firewall data, etc. into the configuration management database to properly segregate the information used for the BSS asset management function. As the result of this control, only the Incident module is used as the customer information collection point for forms and data, no information can be transferred between different modules.

CSC customers may also use the DWP module, which offers an internal web portal for customers to report incidents or to request services. The ticket generated may contain unrequested PII data for the customers. The CSC has a process to review all data to ensure the published documents do not contain PII data to mitigate the relevant privacy risk.

The specific BSS will support the DOI Lumen ESN and DOI-CIRC processes. To mitigate the risk for DOI-CIRC, the PII tab is protected/isolated from the incident itself. Only limited users have access to this information. BSS has designed and implemented separate incident tracking and information display pages for DOI-CIRC and has also disabled the feature of uploading attachments on the main incident form so that no document containing PII can be unnecessarily shared and potentially stored in BSS.

Twice a year, the BSS system support personnel will employ database queries and reporting utilities to extract and review data that may match SSN data structure masks. This data will be reviewed and removed or masked in the system manually if determined that it contains PII.

To mitigate the risk of unauthorized access, access controls are implemented within the BSS System ensuring the least privilege policy are enforced via inheriting the AD directory controls, and the access control measures are being continuously monitored. Role-based access is manually reviewed and audited annually. Additional security measures have been designed and implemented to ensure that only DOI-CIRC administrators, DOI-CIRC bureau users, and privacy officials can access DOI-CIRC incidents within BSS. Additionally, users from each bureau are only entitled to view tickets associated to the bureau in which they are assigned. The BSS incident tracking process for DOI-CIRC also documents and tracks the reported incident information collected by Encase, a forensic tool used for incident investigation. Encase can capture any data of interest residing on a user's computer system, however, these data are not stored in BSS; and have been provided adequate security and privacy controls under the DOI security program.

There is a risk that data in BSS will be maintained for longer than necessary to support the Department's mission, or that records may not be properly destroyed. This risk is mitigated by managing records in accordance with a NARA-approved records schedule. To ensure the BSS records are maintained and disposed of in compliance with the U.S. legal requirements, various record retention and disposition schedules are identified for specific sets of records of BSS. DOI properly defined and assigned roles and responsibilities for the record management and has established record retention and disposition procedures, policy and departmental manual for DOI personnel to follow, thereby mitigate the potential risks that might arise from mishandling of BSS records.

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*

The use of the data is relevant and necessary to provide support to the lines of businesses to process and resolve customer requests in a timely and efficient manner.

☐ 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?

BSS does not derive new data or create previously unavailable data about an individual through data aggregation.

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*

BSS uses a three-tier approach to respond to the customer requests, all incident tickets are triaged by the BSS Tier 1 helpdesk support staff, by either addressing the issue or routing it to Tier 2 support:

Tier 1 Support: This is the Customer Service Center who provides first level of support to end user to obtain incident resolution information. This support covers basic issues such as password resets, software navigation issues, troubleshooting standard software functionality issues, system availability checks/validations, and workflow errors and updates. Issues requiring more extensive expertise are escalated for Tier 2 support. During the escalation and resolution process, customers can contact the CSC Help Desk for a status update or other concerns regarding the incident. Customer POC information such as the name, and email address are collected for issue resolution and follow-up purpose. Once the incident is created, it is then assigned to the appropriate Tier 2 support team for resolution.

Tier 2 Support: The Tier 2 support is provided by application administrators for the applications identified previously. This support covers configuration and network communication issues, application configuration issues, job scheduling, table maintenance, supplier information, application security, issues escalated from Tier 1, or customer requests, such as a missing W-2 as well as other complex issues. The Tier 2 support escalates issues requiring more extensive expertise to the Tier 3 support.

Tier 3 Support: The Tier 3 support requires coordination and interaction with the technical representatives in the applicable bureaus and offices and supporting vendors. Requires in-depth analysis and resolution of application or system problems. BSS administrator also provide Tier 3 support for the BSS application itself when issues with the BSS system occur and for administration of the BSS system.

BSS administrator are the system administrators of the BSS IT Service Level Management system and are responsible for system maintenance and upkeep, code development and deployment and user administration.

User access is determined by roles in the system. System administrators maintain the system and assign the roles and permissions and are responsible for the development efforts for the system. Tier1 (CSC agents) are given a role profile necessary to do their jobs across multiple applications they support. Tier 2 (Support Staff) are given roles to support their particular application/line of business and are placed in support groups to perform these roles.

The BSS users have limited access to the system and are allowed to only submit requests into the system with read-only rights. The customer agency supervisor-level employees and the application support leads approve new user to be setup on the BSS system. Tier 2 managers responsible for application areas authorize the addition of new users in the BSS system as well as changes in BSS which affect their areas of responsibility. The access rights of Tier 2 users require additional levels of approval.

Contractors provide Tier 1 and Tier 2 support across the system have the same access rights as the government employees and are subjected to the same authorization and approval process. The BSS team administers and develops automated solutions to improve customers processes. The BSS team has contractors on board who perform development and maintenance of the system. All changes made by the contractors are reviewed and authorized by responsible government employees.

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

All the modules of the BSS system share the same database and are closely integrated. The user access to the information can only be authorized based on the business need-to-know and least privilege and is constrained by the specific roles of the users. The BSS system uses role level security. Users are granted access based on their specific role within the system for the user organization.

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?*

BMC is the vendor who provides the BSS software and technical support to the BSS team. BMC does not directly access the system, they do however provide direction on development of custom code and maintenance of the system. DOI has a contract with BMC for this ongoing support. The contractor is subject to the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1 and 24.2) and the specified contract clauses (Parts 52.224-1 and 52.224-2) to ensure that personal information processed or maintained by contractors who work on DOI-owned systems of records and the system data are protected as mandated.

Additionally, the following would apply to any contractor of the Federal Government:

- The Privacy Act applies to federal government contractors who operate systems of records containing personal information.
- When an agency contracts for the design, operation, maintenance, or use of systems containing information covered by the Privacy Act, the contractor and its employees are

considered employees of that agency and are subject to the same requirements for safeguarding information as Federal employees.

- The contractors and their employees also are subject to civil and criminal sanctions under the Act for any violation that may occur due to oversight or negligence.

BSS administrator contractors as well as Tier 1 and Tier 2 support personnel are subject to the same rules and regulations as government employees.

☐ 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*

BSS maintains audit logs of actions of the users in the system.

☐ No

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

Login, failed login, login date, actions in the system and changes such as the changes to a record for Tier 1 and Tier 2 staff are recorded in an application audit log.

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

Access controls are implemented to comply with the least privilege policy to prevent unauthorized monitoring, as inherited by AD controls that reside within the OCIO. Levels of access are manually reviewed annually to ensure appropriate access for users dependent on their role. System access is controlled through roles and permissions within the application. The system administrator users must have a license and permission to view audit log information. Typically, all Tier 1 and Tier 2 support personnel can review the audit log information.

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*

(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*

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 Chief, Hosting Services Branch, Service Delivery Division, OCIO serves as the BSS System Owner and the official responsible for oversight and management of the BSS security controls and the protection of customer agency information processed and stored by the BSS system.

The Information System Owner and data owners 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 BSS and accessed by authorized staff in the supporting systems. They are also responsible for protecting the privacy rights of the employees, volunteer workers, and customers for the information they collect, maintain, and use in the system. The Privacy Act System Managers and data owners for the supported Privacy Act systems are responsible for meeting the requirements of the Privacy Act, providing adequate notice, making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with appropriate Privacy Officials.

Customer agency data in BSS is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints.

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 BSS Information System Owner has responsibility for daily operational oversight and management of the BSS 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 BSS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the appropriate Privacy Officials.