U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior (DOI) requires Privacy Impact Assessments (PIA) be conducted and maintained on all IT systems whether already in existence, in development, or undergoing modification in order to 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: Safety Management Information System (SMIS)
Date: October 1, 2021

Point of Contact
Email: OS_privacy@ios.doi.gov
Name: Danna Mingo, OS Departmental Offices, Associate Privacy Officer
Phone: (202) 441-5504
Address: 1849 C Street, NW, Room 7112, Washington, D.C. 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:

B. What is the purpose of the system?

The SMIS is a web-based system managed by the DOI Office of Occupational Safety and Health (OSH). SMIS is the Department's official accident, injury and illness reporting, analysis and recordkeeping system for DOI employees, contractors, volunteers, and visitors to DOI facilities. SMIS helps the Department comply with the Department of Labor (DOL) Occupational Safety and Health Administration's (OSHA) regulations, mandates and requirements (29 CFR 1960), Basic Program Elements for Federal Employees, which require that agencies maintain recordkeeping systems for proper evaluation and necessary corrective action, and to develop and

maintain an effective program of collection, compilation, and analysis of occupational safety and health statistics. The SMIS application provides the functionality to support business processes within DOI, bureaus, and offices that enhance the health and safety of employees, contractors, volunteers and visitors.

The main module of SMIS documents near misses, exposures, and incidents within the Office of the Secretary (OS), Bureau of Land Management (BLM), Bureau of Indian Affairs (BIA), Bureau of Indian Education (BIE), Bureau of Reclamation (BOR), United States Geological Survey (USGS), Bureau of Ocean Energy Management (BOEM), National Park Service (NPS), US Fish and Wildlife Service (FWS), , Office of Surface Mining Reclamation and Enforcement (OSMRE), Bureau of Safety and Environmental Enforcement (BSEE), and Bureau of Trust Funds Administration. The system has a web-based interface that allows users to login and enter the required information. Safety managers are then able to review incident information to fulfill OSHA reporting requirements and to develop strategies to prevent similar incidents from occurring in the future.

SMIS has an Inspection and Abatement (IAS) module utilized by BOR, BLM, and USGS. The IAS module is a tool for bureaus to generate inspection checklists and digitally record safety inspections for their respective facilities.

In September 2021, a separate module was added to SMIS to support a new system of records for the collection of information on employee vaccination for COVID-19 disease. This new module contains the DI-6507, Vaccination Requirement for DOI Employees Form that will collect dates and types of vaccine as well as proof of vaccination directly from DOI Federal employees as required by Executive Order 14043, *Requiring Coronavirus Disease 2019 Vaccination for Federal Employees*, signed September 9, 2021, which establishes mandatory requirements for Federal executive agencies to implement a program to require COVID-19 vaccinations for Federal employees, with some exceptions as required by law. This vaccination program will help DOI manage records related to DOI's response to COVID-19, support emergency or medically related decisions affecting DOI personnel, and ensure the health and safety of DOI's workforce. DOI will only collect the minimum information necessary to comply with Federal workforce safety requirements.

This privacy impact assessment (PIA) evaluates privacy risks for the collection and use of personally identifiable information for the separate modules in SMIS and will be updated as processes or information collections change, or the system is modified.

C. What is the legal authority?

The Occupational Safety and Health Act of 1970, Section 19, 29 U.S.C. § 668; Health Service Program, 5 U.S.C. § 7901; 5 U.S.C. §§ 2671-2680; 31 U.S.C. §§ 240-243; Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters, 29 CFR 1960; and Executive Order 12196, Occupational Safety and Health Programs for Federal Employees.

In addition to the above, the collection of vaccine information is covered under 5 U.S.C. chapters 11 and 79, and in discharging the functions directed under Executive 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (September 9, 2021) and 5 U.S.C. chapters 33 and 63, 25 U.S.C. 2012, Indian Education Personnel, and Secretarial Order 3402, COVID-19 Vaccine Mandate for Educators at Bureau of Indian Education-Operated Schools.

This system supports DOI's COVID-19 response and management of employee vaccination records as required by Executive Orders (EO) 13991, Protecting the Federal Workforce and Requiring Mask-Wearing; Office of Management and Budget (OMB) Memorandums M-21-15, COVID-19 Safe Federal Workplace: Agency Model Safety Principles, and M-21-25, Integrating Planning for A Safe Increased Return of Federal Employees and Contractors to Physical Workplaces with Post-Reentry Personnel Policies and Work Environment; COVID-19 Workplace Safety: Agency Model Safety Principles issued by the Safer Federal Workforce Task Force; and other applicable law and policy. Federal labor, employment and workforce health and safety laws that govern the collection, dissemination, and retention of DOI employees' medical information include the Americans with Disability Act (ADA) and the Rehabilitation Act of 1973 (Rehab Act). The HHS Secretary may, under section 319 of the Public Health Service (PHS) Act (codified at 42 U.S.C 247d, declare that: (a) A disease or disorder presents a public health emergency; or (b) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists.

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:

E. Is this information system registered in CSAM?

☒ Yes: UII Code - 010-000000708; Safety Management Information System (SMIS) Security and Privacy Plan

☐ 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.*
Safety Net	General bureau safety information	No	N/A

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

☒ Yes:

The workplace injury or illness reporting and workers compensation records in SMIS are covered under DOI-60, Safety Management Information System, October 24, 2016 (81 FR 73135) and government-wide records notice DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File, April 29, 2016 (81 FR 25776). Some records may be covered under DOI-85, Payroll, Attendance, Retirement and Leave Records, July 19, 2018 (83 FR 34156); OPM/GOVT-1, General Personnel Records, December 11, 2012 (77 FR 79694), modification published at November 30, 2015, (80 FR 74815); and OPM/GOVT-10, Employee Medical File System Records, June 21, 2010 (75 FR 35099); modification published November 30, 2015 (80 FR 74815). These notices may be viewed on the DOI SORN page at https://www.doi.gov/privacy/sorn.

The Vaccination Requirement for DOI Federal employee records are maintained is a separate module in SMIS. These employee vaccination records are covered by OPM/GOVT-10, Employee Medical File System Records, December 11, 2012 (77 FR 79694), modification published November 30, 2015, (80 FR 74815), which covers Federal employees defined by 5 U.S.C. Chapter 21. A new SORN is being developed to support a comprehensive workplace vaccination program for Title 25 employees as defined by 25 U.S.C. 2012 and any non-Title 5 civil service employees that are not covered by the OPM/GOVT-10 SORN.

☐ No

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

☐ Yes:
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Gender
☒ Birth Date
☒ Truncated SSN
☒ Medical Information
☒ Disability Information
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other:

In addition to the PII above, the SMIS workplace injury, illness and workers compensation module in SMIS also contains date of injury, date of death, injury code, and illness, accident or injury data for DOI employees, contractors, and volunteers. Information collected about workplace accidents, injuries or illness, and workers' compensation claims include occupation code, Office of Workers' Compensation Programs (OWCP) case number, OWCP adjudication code, OWCP case status codes, OWCP medical costs, OWCP compensation costs, DOI employee salary information, a summary of the accident and/or injury or illness related to the worker's compensation claim for analytical purposes, and a descriptive narrative about the cause of the accident, injury or illness, and/or worker's compensation claim information.

The system previously collected injury/illness data on visitors to DOI facilities however, the system no longer collects this data. The last 3 years of records are still in the system and will be disposed of in accordance to the record disposition authority.

PII in the Vaccination module will be limited to employee name, dates of vaccination, type of the vaccine, and an uploaded copy of any of the following records of vaccination:

1. Record of immunization from a health care provider or pharmacy; or
2. COVID-19 Vaccination Record Card (Centers for Disease Control and Prevention (CDC) Form MLS-319813published on September 3, 2020); or
3. Medical records documenting the vaccination; or
4. Immunization records from a public health or state immunization information system; or
5. Any other official documentation containing required data points (date(s) of vaccine, who administered the vaccine, type of vaccine, name of employee, date of birth)

The vaccination form workflow includes employee name and email address and supervisor name and email address.

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*

Data from the SMIS workplace injury and accident module is imported from Federal Personnel and Payroll System (FPPS), DOL, SMIS users, supervisors, safety managers performing updates and approvals, and workers compensation coordinators.

The vaccination module information is collected directly from the Federal employee through the DI-6507 form.

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

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Web site https://www.smis.doi.gov/
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems:
☒ Other:

For the SMIS workplace injury and accident module:

1) Personnel data on DOI employees is imported from FPPS.

2) DOL provides quarterly case payment (chargeback) data.

3) SMIS users, supervisors, safety managers performing updates and approvals, workers compensation coordinators, can enter data into the system via the internet.

For the Vaccination module, information is obtained directly from the Federal employee through the DI-6507 form.

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

The PII collected is necessary to comply with DOL OSHA regulations and standards, 29 CFR Part 1960, Basic Program Elements for Federal Employees, which requires that agencies maintain recordkeeping systems for proper evaluation and corrective action, and to develop and maintain an effective program for collection, compilation, and analysis of occupational safety and health statistics.

PII is used to report and analyze accidents, injuries, illnesses, and exposures that happen within the DOI. The collected information is updated as the incident is investigated. The information collected as part of this process can be leveraged to provide updated policies and help case managers track, review, and monitor incidents that require workers compensation payments.

For the Vaccination module, the vaccine information collected is used to maintain and promote the safety of Federal workplaces and the Federal workforce referenced in Section 2C. of this PIA, Executive Order 13911, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan 20, 2021), Executive 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (September 9, 2021), The COVID-19 Workplace Safety; Agency Model Safety Principles established by the Safer Federal Workforce Task Force, Secretarial Order 3402, COVID-19 Vaccine Mandate for Educators at Bureau of Indian Education-Operated Schools, and guidance from CDC and the OSHA.

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

☒ Within the Bureau/Office:

For the SMIS workplace injury and accident module, SMIS provides reporting and Key Point Indicators (KPI) for all aspects of the incident information collected. This includes incident cost, Department incident rates, OSHA-specific reporting, and ad-hoc requests. Organizational and Departmental statistics are used by Departmental leadership for tracking trends and identifying areas where safety program weaknesses need to be addressed. Reports on individual incidents are provided to Bureau Safety Managers and Compensation Coordinators to help them better manage incidents that resulted in OWCP cases.

For the Vaccination module, PII may be shared internally with supervisors, Human Resources personnel, and authorized personnel for the purpose of validating vaccination status, managing vaccination documentation, and meeting Federal requirements.

☒ Other Bureaus/Offices:

The SMIS workplace injury and accident module provides reporting and KPI's for all aspects of the incident information collected. This includes incident cost, Department incident rates, OSHA-specific reporting, and ad-hoc requests. Bureau and Departmental statistics are used by departmental leadership for tracking trends and identifying areas where safety program weaknesses need to be addressed. Reports on individual incidents are provided to Bureau Safety Managers and Compensation Coordinators to help them better manage incidents that resulted in OWCP cases.

For the Vaccination module, PII may be shared with the Departmental officials and with bureau and office supervisors, Human Resources personnel, and authorized personnel for the purpose of validating vaccination status, managing vaccination documentation, and meeting Federal requirements.

☒ Other Federal Agencies:

The SMIS workplace injury and accident module provides reporting and KPI's for all aspects of the incident information collected. This includes incident cost, Department incident rates, OSHA-specific reporting, and ad-hoc requests. Bureau and Departmental statistics are used by Departmental leadership for tracking trends and identifying areas where safety program weaknesses need to be addressed. Reports on individual incidents are provided to Bureau Safety Managers and Compensation Coordinators to help them better manage incidents that resulted in workers compensation payments.

PII is shared with DOL as required by regulation in order for compensation claims to be assigned a claim number, and to provide quarterly listings of fatalities, disabling injuries, illnesses and property damage. Information related to accidents, injuries, illness, investigations and claims may also be shared with other Federal agencies and organizations as authorized and identified in the published routines uses in DOI-60, Safety Management Information System. Some information in SMIS is also covered by government-wide system notices DOL/GOVT-1, Federal Employees' Compensation Act File, OPM/GOVT-1, General Personnel Records, and OPM/GOVT-10, Employee Medical File System Records. These notices may be viewed on the DOI Privacy Program SORN page: https://www.doi.gov/privacy/sorn.

For the Vaccination module, information may be shared with the Office of Personnel Management (OPM), other Federal agencies as necessary to comply with laws governing the reporting of communicable disease or the health and safety of the workforce; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or other organizations and entities as outlined in the routine uses in the published OPM/GOVT-10, Employee Medical File System Records, SORN.

☒ Tribal, State or Local Agencies:

For the Vaccination module, information may be shared with a state or local agency as necessary to comply with laws governing the reporting of communicable disease or the health and safety of the workforce, or other organizations and entities as outlined in the routine uses in the published SORN, OPM/GOVT-10, Employee Medical File System Records.

☒ Contractor:

For the SMIS workplace injury and accident module, contractors are used for development on the SMIS application and helpdesk. The helpdesk position is required to have full access to SMIS data and reporting. The development positions are given access to reporting when needed but do not access production data regularly.

For the Vaccination module, information may be shared with DOI contractors who are authorized to perform their duties for the Federal Government and access will be based on least privileges.

☒ Other Third-Party Sources:

For the SMIS workplace injury and accident module, PII may be shared with other organizations to facilitate the functions of the SMIS application and claims processes as authorized and identified in published routines uses in the DOI-60, Safety Management Information System and government-wide records notice DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File. Some records may be covered under DOI-85, Payroll, Attendance, Retirement and Leave Records, OPM/GOVT-1, General Personnel Records, and OPM/GOVT-10, Employee Medical File System Records. These notices may be viewed on the DOI SORN page at https://www.doi.gov/privacy/sorn.

For the Vaccination module, information may be shared with courts, entities and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement as outlined in the routine uses in the published system of records notice, OPM/GOVT-10, Employee Medical File System Records.

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

☒ Yes:

For the SMIS workplace injury and accident module, individuals choose to voluntarily provide information when reporting accidents, injury or illness directly in SMIS. The SMIS home page contains a Privacy Act Statement that informs the individual of the authority, purpose, routine use, voluntary nature, and the impact for not providing the requested information.

For the Vaccination module, employees have the opportunity to voluntarily provide their vaccination information and documentation. Providing vaccine information is mandatory for DOI Federal employees under E.O. 14043 and S.O. 3402, subject to limited legal exception under the law for reasonable accommodations due to medical reasons or religious belief, practice, or observance. Employees are notified that failure to provide the information requested may result in appropriate corrective action, up to and including removal from federal service.

A Privacy Act statement is provided on the DI-6507 form that informs individuals of the authority, purpose, specific uses of information, authorized disclosures, and the voluntary nature of the collection of their vaccination status and any impacts for not providing their status. This allows individuals to make informed decisions on the provision of their information. DOI will provide a Privacy Act statement for non-Title 5 employees once the DOI SORN is published.

☐ No:

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

☒ Privacy Act Statement:

A Privacy Act statement is provided for the workplace injury, illness and workers compensation module in SMIS:

This information is being solicited under the authority of the Occupational Safety and Health Act of 1970, Section 19, 29 U.S.C. 668; Health Service Program, 5 U.S.C. 7901; 31 U.S.C. 3721; Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters, 29 CFR 1960; and Executive Order 12196, Occupational Safety and Health Programs for Federal Employees. The primary purpose of this system is to record and maintain information on accidents, injuries and illnesses incurred by DOI employees, contractors, volunteers and visitors. SMIS maintains information on workplace injuries, workplace illness, and workers' compensation claims; provides summary data of injury, illness and property loss information for analytical purposes to improve accident prevention policies, procedure, regulations, standards, and operations; provides listings of individual cases to ensure that accidents are reported as appropriate; and assist OWCP in the adjudication of employee worker's compensation claims. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as found in the published system of records notice, DOI-60, Safety Management Information System (SMIS) - 81 FR 73135 (October 24, 2016), which may be viewed at: https://www.doi.gov/privacy/sorn. The effect on the individual of not providing all or any part of the requested information may be to render impossible or to delay the Department's documenting the injury and/or property loss. Every effort will be made to obtain the factual information relating to an incident from other sources, should the individual involved refuse to provide the requested information.

The following Privacy Act Statement is provided on the DI-6507 form in the Vaccination module in SMIS:

Authority: Pursuant to 5 U.S.C. chapters 11 and 79, and in discharging the functions directed under Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (Sept. 9, 2021), we are authorized to collect this information. The authority for the system of records notice (SORN) associated with this collection of information, OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), also includes 5 U.S.C. chapters 33 and 63 and Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980). Providing this information is mandatory, and we are authorized to impose penalties for failure to provide the information pursuant to applicable Federal personnel laws and regulations.

Purpose: This information is being collected and maintained to promote the safety of Federal workplaces and the Federal workforce consistent with the above-referenced authorities, Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.

Routine Uses: While the information requested is intended to be used primarily for internal purposes, in certain circumstances it may be necessary to disclose this information externally, for example to disclose information to: a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of communicable disease or other laws concerning health and safety in the work environment; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to contractors, grantees, or volunteers as necessary to perform their duties for the Federal Government; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or to a person authorized to act on your behalf. A complete list of the routine uses can be found in the SORN associated with this collection of information.

Consequence of Failure to Provide Information: Providing this information is mandatory. The failure to provide this information may result in appropriate corrective action, up to and including removal from federal service.

A Privacy Act statement will be provided for non-Title 5 employees once the DOI SORN is published.

☒ Privacy Notice:

For the SMIS workplace injury and accident module, notice is also provided in the following SORNS: DOI-60, Safety Management Information System and DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File. Some records may be covered under DOI-85, Payroll, Attendance, Retirement and Leave Records,

OPM/GOVT-1, General Personnel Records, and OPM/GOVT-10, Employee Medical File System Records. These notices may be viewed on the DOI SORN page at https://www.doi.gov/privacy/sorn.

This SMIS PIA has been developed to allow DOI to communicate more clearly with the public about how we handle information, including how we address privacy concerns and safeguard information. DOI PIAs may be viewed at https://www.doi.gov/privacy/pia.

For the Vaccination module, individuals are provided notice through the publication of this PIA and the OPM/GOVT-10, Employee Medical File System of Records, SORN.
☐ Other:

☐ None

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

The SMIS workplace injury and accident module has primary fields used for retrieving data including date, incident ID, name, audit ID, facility name, and case number for legacy data and the IAS module.

For the Vaccination module, User Identifier (32-character ID from DOI Talent) will be the primary key used to retrieve data from the Vaccination Forms under the new module in SMIS.

I. Will reports be produced on individuals?

☒ Yes:

The SMIS workplace injury and accident module generates reports on single individual cases, payments made, reports for organizations that show statistics on personal and property accidents and injuries, and reports that show accident and injury statistics for DOI-wide. Reports on individual cases are used by Safety Managers and Compensation Coordinators to track completion of activities on individual cases. Reports for organizational and DOI statistics are used by organizations, DOI Safety Managers, and the DOL-OWCP for tracking trends and identifying areas where safety program weaknesses need to be addressed.

The Vaccination module, reports may be developed by authorized human resources and health and safety officials on employee completion status for the form and vaccination status. Reports with aggregated metrics may also be produced, such as reports on number of employees vaccinated, number of partially vaccinated, and number of forms completed, that will not identify specific individuals. Reports will be used to oversee and manage the system, ensure records are accurate, and meet reporting requirements. Only authorized users will have access to generate or view reports. The system owner and responsible officials are required to ensure

reports that contain PII are safeguarded and sharing is limited to authorized personnel with an official need to know.

☐ No

Section 3. Attributes of System Data

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

For the SMIS workplace injury and accident module, data entered into the SMIS workplace injury and accident module goes through verification via built in features within the application. All fields are checked for errors before the user can complete the form and post the data to the database. Data that is imported into SMIS goes through the same verification process and is flagged for review by the SMIS team.

For the Vaccination module, information is obtained directly from employees who are responsible for validating the information prior to submitting the information in the system.

B. How will data be checked for completeness?

For the workplace injury and accident module, information is generally collected directly from individuals. SMIS users are asked standardized questions regarding their incident. Based on the responses to those questions, the application builds the requirements for completion of the incident report. The SMIS application requires the user to complete all required fields within a form before moving on to the next section of the incident report. The incident report can only be posted to the database upon completion of all sections of the incident report, review by the supervisor, initial review by the first line safety manager, and final review by the Regional Safety Manager.

For the Vaccination module, information is obtained directly from the employees who are responsible for ensuring the completeness of their responses. The employee's supervisor has the responsibility to validate the information submitted by their employees. The SMIS vaccine module includes error message that must be mitigated before the employee is able to submit their Vaccine Form.

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

For the SMIS workplace injury and accident module, users are required to enter incident data into SMIS within 48 hours of the incident. Email reminders are sent out to safety managers with reminders about actions needed from them to complete the incident. Compensation data is imported and verified quarterly. Chargeback data is imported in time to for safety managers to meet OSH reporting deadlines.

For the vaccination module, information on employee vaccination status is collected directly from employees through the DI-6507 form. Employees can update their status at any time by accessing their records in the Vaccination module and submitting a new form. Employees can also contact their supervisor to update their record. Authorized personnel will utilize system and manual functions to ensure the system and program uses the latest submission on vaccination status as the current record.

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

For the SMIS workplace injury and accident module, records in this system including forms, reports, correspondence, and related medical and investigatory records concerning on-the-job injuries, are maintained under Departmental Records Schedule (DRS) 1.2A - Short-Term Human Resources, which has been approved by NARA (DAA-0048-2013-0001-0004). The disposition for these records is temporary and the records are cut-off on termination of compensation or when the deadline for filing a claim has passed. Records are destroyed three years after cut-off.

Records that include investigative case files of fires, explosions, and accidents submitted for review and filing in other agencies or organizational elements, and reports and related papers concerning occurrences of such a minor nature that they are settled locally without referral to other organizational elements and not covered by DRS-1.2A are maintained under DRS-1.1A, Short-Term Administration Records (DAA-0048-2013-0001-0001). The disposition for these records is temporary and the records are cut-off at the end of the fiscal year in which the records are created. Records are destroyed three years after cut-off.

Records related to motor vehicle accidents maintained by transportation offices are maintained under DRS-1.1B, Long-Term Administration Records (DAA-0048-2013-0001-0002). The disposition for these records is temporary and the records are cut-off at the end of the fiscal year in which files are closed. Records are destroyed seven years after cut-off.

For the Vaccination module, records related to employee vaccinations will be maintained in accordance with GRS 2.7 / 060, Occupational individual medical case files. The disposition for these records is temporary. Destroy 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer. (DAA-GRS-2017-0010-0009).

System administration records are maintained under the Departmental Records Schedule (DRS)-4.1, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the bureaus/offices activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three years after cut-off.

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

Prior to any deletion of records in SMIS, submission and approval of a DI-1941 is required. SMIS records will be hard deleted from the SMIS production system. The criteria for deletion is documented. Deletion of records is an automated process that runs monthly and hard deletes the record from production data.

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 is a moderate risk to the privacy of individuals due to the sensitive PII contained in the system. SMIS is used to collect workplace accident, injury and illness data to assist Department executives, safety managers, and frontline DOI employees manage safety risks. Most of the data in SMIS is collected and entered by the individuals involved in the accident, injury or illness, or a supervisor or safety manager.

SMIS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) guidelines. SMIS is 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 sensitive PII contained in the system. Appropriate privacy and security controls have been implemented to safeguard PII and prevent unauthorized access, use or disclosure of records maintained in SMIS in accordance with Federal laws, regulations, and policy.

SMIS has limited file transfer with two (2) partners: FPPS, an internal DOI personnel system, and DOL, an external Federal agency partner. User ID and password are required to gain access to the respective systems for both of these limited file transfers.

SMIS applies the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. An audit trail of activity sufficient to reconstruct security relevant events is maintained and includes 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, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. DOI employees and contractors are

required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system are required to take additional role-based training and sign DOI Rules of Behavior.

Records are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. Paper records are maintained in locked file cabinets under the control of authorized personnel in secured DOI controlled facilities with physical, technical and administrative levels of security to prevent unauthorized access to DOI information assets. Computer servers on which electronic records are stored are in secured DOI facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information systems. Security controls to protect the DOI network and information systems include encryption, firewalls, audit logs, and network system security monitoring.

The Vaccination module will be used to collect and maintain information concerning the vaccine status of DOI Federal employees. There may be a risk that employees may not receive notice or opportunity to consent to collection or use of information. This risk is mitigated by the Privacy Act statements provided to employees that explain the purpose and uses of information, and the publication of this PIA and the OPM/GOVT-10 SORN, which also provides guidance to employees on how they can seek redress, access or amendment of their records. The DOI Privacy Program website also provides guidance to individuals on how to submit a Privacy Act request or complaint.

There is a risk that the system may collect, store or share more information than necessary for an official business need, the information may be used for an other than authorized purpose, or that data may be incorrect or subject to unauthorized alteration that may subject individuals to adverse action or penalties. Access to data is restricted to authorized personnel to perform official functions. Data collected and maintained is limited to the minimal amount of data needed to meet Federal requirements for ensuring the health and safety of the Federal workforce. The authorized human resources and health and safety officials will not change the actual responses submitted by individuals. The system also provides audit processes to track changes. Authorized officials must complete role-based training and acknowledge rules of behavior to ensure an understanding of their responsibilities for using and sharing data only for authorized purposes.

There is a risk of unauthorized access or disclosure of records or reports that contain PII, which may reveal details of an individual's vaccination status and lead to harm or embarrassment to the individual. Employee medical files must be maintained in accordance with OPM regulations, 5 CFR part 293 subpart E, and OPM/GOVT-10, Employee Medical File System Records. These records must be maintained separately from the Official Personnel Folder. Records may only be accessed by authorized human resources personnel, health and safety personnel, system administrators, and supervisors who have an official need to know to perform their duties. The Vaccination module may only be accessed with a PIV card while on the VPN from within the

DOI network. For employees without a PIV card or network access, their supervisor will work with them to complete the form and meet the vaccination document requirement. Each bureau will develop a plan to assist the impacted employees in securely submitting information.

SMIS has a module that contains a Vaccine Form that allows the employees to upload the image of their documentation that validates their vaccine. There is a privacy concern that an employee can inadvertently upload a wrong image that could impact the privacy of the employee and or family members. The image can be "soft deleted" which marks the record as inactive and won't be visible to employee or supervisors.

There is a risk that supervisors can download the vaccine card or medical document of employees, however, the SMIS system owner and the Office of Human Capital will provide instructions to the supervisor regarding their responsibilities in protecting the sensitive PII. The managers have been assigned Role-Based Privacy Training that outlines their responsibilities to protect the data under their authority.

There is a risk that PII collected by this system may be retained longer than necessary. Records are maintained and disposed of under a NARA approved records schedule. Information collected and stored within SMIS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. The data collected and stored is limited to the minimum amount of data needed to meet Federal requirements and protect the Federal workforce. Users are reminded through policy and training that the applicable retention schedules must be followed. Responsible officials will work with records management officials to ensure records are retained and disposed of in accordance with the records retention schedule and the Federal Records Act.

The Vaccination module applies the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. An audit trail of activity sufficient to reconstruct security relevant events is maintained and includes 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, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system are required to take additional role-based training and sign DOI Rules of Behavior.

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:

For the SMIS workplace injury and accident module, data collection is used by Bureau safety managers OSH staff to minimize future injuries, illnesses, and fatalities. Bureaus also use SMIS to complete required annual OSHA reporting. SMIS data helps compensation coordinators manage CA1 and CA2 cases to lower costs associated with workers compensation.

For the Vaccination module, the vaccine information is being collected to maintain and promote the safety of Federal workplaces and the Federal workforce referenced in Section 2C. of this PIA, Executive Order 13911, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan 20, 2021), The COVID-19 Workplace Safety; Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not applicable. SMIS 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.

☐ Yes, processes are being consolidated.

☒ 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:

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

For the SMIS workplace injury and accident module, all SMIS users are only given access to data that is required for them to complete their duty given their role within the DOI. A supervisor must complete an on-screen form to request user accounts.

For the vaccine module, all DOI Federal employees who have a PIV card will have access to the DI-6507 Vaccination form in order to fulfill the requirement mandated under the Executive Order. Access to the records is strictly limited to authorized personnel who have a need to know to perform their official duties based on the least privilege principle. The responsible human resources and health and safety officials designate specific users based on their roles to perform functions in the system. Authorized users must take initial and annual privacy and security training, role-based training, and must acknowledge and adhere to the DOI rules of behavior.

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.

Contractors are involved in the design, development, and maintenance of the system. Privacy Act clauses are included in the contract for SMIS.

☐ 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.

☒ No

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

☒ Yes.

For the SMIS workplace injury and accident module, SMIS monitors user actions within the system. Log tables have been implemented that track who made changes to the data and what changes that user made. Failed and successful login attempts are logged with the IP those attempts were made from. Changes to data within the system are logged along with the user that made the changes.

☐ No

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

SMIS collects all information around logins including IP address, user email, user ID, and number of attempts. Any create, update, or delete action within the system is logged with a time stamp and user ID.

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

For the SMIS workplace injury and accident module, the SMIS system complies with NIST and other Federal requirements for data security as part of the formal program of assessment and authorization, and continuous monitoring. Weekly 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 SMIS equipment. The use of DOI IT systems, including SMIS, is conducted in accordance with the appropriate DOI use policy. An audit trail of activity is maintained to reconstruct security relevant events that includes 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.

For the Vaccination module, access to the records is strictly limited to authorized personnel who have a need to know to perform their official duties. The responsible human resources and health and safety officials designate specific users based on their roles to perform functions in

the system. Authorized users must take initial and annual privacy and security training, role-based training, and must acknowledge and adhere to the DOI rules of behavior.

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.

(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.

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 SMIS System Owner within the DOI Office of Occupational Safety and Health is responsible for oversight and management of security and privacy controls and the protection of agency information processed and stored in SMIS. The SMIS System Owner and the SMIS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy and addressing Privacy Act requests and complaints, in accordance with Federal laws, regulations, and DOI policy for the data managed and stored in SMIS, in coordination with the Departmental Privacy Officer. Each bureau/office program utilizing the SMIS workplace injury and accident module will be responsible protecting the privacy rights of the public and employees, addressing Privacy Act complaints and requests for redress or amendment of records within their authority.

For the Vaccination module, the System Owner and Privacy Act System Manager are responsible for ensuring oversight of the system of records and implementing appropriate safeguards to protect the employee medical records, as well as responding to Privacy Act requests and complaints. All supervisors and authorized personnel are responsible for safeguarding employee privacy and protecting the vaccination records and PII in the 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 SMIS Information System Security Officer is responsible for oversight and management of the SMIS security and privacy controls, and for ensuring to the greatest possible extent that SMIS data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Security Officer is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI breach reporting procedures. Each bureau/office program, supervisor and authorized official utilizing the modules in SMIS will be responsible for ensuring the security of data maintained in SMIS, and for meeting privacy and security requirements within their organization and immediately reporting any potential compromise of data in accordance with Federal and DOI privacy breach response policy.