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: Employee Certification of Vaccination Program
Date: September 17, 2021
Bureau/Office: Office of the Secretary (OS)/Office of Human Capital

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, 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:

B. What is the purpose of the system?

The Office of Management and Budget (OMB) issued guidance requiring Federal agencies to collect the vaccination status of Federal employees to implement safety measures and protect the Federal workforce pursuant to Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.

Agencies are required to ask about the vaccination status of Federal employees to implement and manage the different safety protocols for individuals who are fully vaccinated and those who are not fully vaccinated. The Department of the Interior (DOI) Office of Human Capital is establishing a Department-wide program for determining the vaccination status of employees to ensure appropriate safety protocols based on employees' vaccination status, fully vaccinated or not fully vaccinated, consistent with guidance from the Centers for Disease Control Prevention (CDC) and the Safer Federal Workforce Task Force. Information about the guidance on vaccinations may be viewed on the Safer Federal Workforce Task Force website at https://www.saferfederalworkforce.gov/faq/vaccinations/.

A government-wide template form was developed for agency use to collect vaccination status from Federal employees. The Employee Certification of Vaccination form requires federal employees to provide their vaccination status or decline to provide their status, and attest to the truthfulness of the responses they provide. Providing vaccination status is voluntary. Employees who disclose that they are unvaccinated or decline to complete the attestation will be treated as not fully vaccinated for purposes of implementing safety measures, including requirements for mask wearing, physical distancing, testing, travel, and quarantine.

DOI is taking a phased approach to implement this program and collect vaccination status and other information to reduce the spread of COVID-19 and protect the Federal workforce. Based on existing inventory of available systems, DOI leadership and Office of Chief Information Officer (OCIO) identified the OCIO Microsoft Office 365 Form feature to create an automated Employee Certification of Vaccination form. All responses will be captured in a spreadsheet and stored in a dedicated OneDrive file management system managed by Office of Human Capital until the Department implements a long-term solution to maintain employee medical records related to vaccination status, testing, and other related information required to effectively implement health and safety regulations and Federal safer federal workforce guidance for agency response to COVID-19 disease. The Employee Certification of Vaccination form will be stored in a dedicated and restricted OneDrive file location with limited and controlled access to protect the confidentiality of the employee medical files.

The Microsoft Office 365 Cloud system is a Software as a Service (SaaS) solution providing DOI an enterprise-wide suite of communication, collaboration and office productivity applications. It includes Forms and OneDrive for Business (ODfB). Forms is a web-based application in O365 that allows users to create forms such as surveys, quizzes, and polls with internal users within the DOI environment. Form creators are responsible for setting the appropriate access permissions for their forms. Each form owner is responsible for assessing and managing privacy risks related to collection, use, and dissemination of PII, and following applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.

ODfB is a cloud-based storage repository that facilitates creation, storage, sharing, and collaborative work for all types of electronic files which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information and other confidential information. The files in ODfB are private by default and can only be viewed by the

file creator. OCIO dedicated a new user account for the Office of Human Capital to help capture data from the Microsoft Office 365 Form system to immediately track data responses and begin transferring vaccination-related data to DOI's Safety Management Information System that is situated in DOI's Office of Occupational Safety and Health (OSH). DOI conducted a privacy impact assessment (PIA) to evaluate the privacy implications for use of the Microsoft Office 365 Cloud, which may be viewed at https://www.doi.gov/privacy/pia#DW.

This PIA is being conducted to identify privacy risks associated with DOI's use of the Employee Certification of Vaccination form and the program for the collection, maintenance and processing of information collected from Federal employees on vaccination status, to ensure appropriate privacy controls are implemented to protect individual privacy. DOI will update this PIA as the program and related processes are established, the data collection changes, and the supporting system is developed.

C. What is the legal authority?

Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.

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:
☒ No

This PIA is being conducted to document the privacy risk of the electronic collection of the employee certification vaccination form and the impacts of the program.

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.*
HRIS-BI SQL Database	The OHC HRIS Business Intelligence (HRIS BI) is a SQL Server 2012 database, managed by OHC HRIS, that is used to extract, transform, load and stage human capital data for use as the source for DOI workforce reporting, data analytics and interactive visualizations.	Yes	User Principal Name (UPN); Name; Time Stamp; Vaccine Status; Supervisor Name

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

☒Yes:

OPM/GOVT-10, Employee Medical File System Records, 75 FR 35099 (June 21, 2010); modification published at 80 FR 74815 (November 30, 2015)

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Medical Information
☒ Employment Information
☒ Other:

Information collected from employees through the automated form includes employee name, official email address, vaccination status - fully vaccinated, not yet fully vaccinated, not vaccinated, or decline to respond, an employee attestation to truthfulness of responses,

supervisor's name and email address, date of submission. Name, email address, form entry start date/time and form completed date/time are captured as part of the automated form submission. To ensure data accuracy, the responses and attestations submitted by employees will not be revised by officials, however employees may update their status at any time. Human resources officials may use the responses provided and additional information from other existing DOI records to include bureau/office, sub-bureau/office, organization, employee common identifier (ECI) that is used in lieu of Social Security numbers (SSNs), assigned supervisor, employee appointment type, and employment status, to verify the current supervisor and support system management and required reporting.

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:

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: FPPS, DOI Talent, and Active Directory
☒ Other:

The Employee Certification of Vaccination form is disseminated to all employees via their official email address with a link to the form. Employees will submit responses through the automated form and may use the same link to submit additional forms to provide their updated status. In limited circumstances where an employee does not have an official email address or network access, responsible officials will determine appropriate methods of delivery and submission including paper or email.

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

DOI is implementing the Employee Certification of Vaccination form in accordance with OMB guidance to prevent the spread of COVID-19 and protect the health and safety of all Federal

employees. Federal employees are required to complete the form and attest to their vaccination status or may decline to provide their vaccination status.

The information collected is used to promote the safety of Federal buildings and the Federal workforce in accordance with Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.

The requested information will help DOI implement safety measures to protect its workforce consistent with the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, guidance from the CDC and the Occupational Safety and Health Administration and comply with laws governing communicable disease or the health and safety of the work environment. DOI officials will use the information to determine access to DOI controlled buildings, facilities, workspace, meetings, conferences, events, and enforce requirements for mask wearing, physical distancing, testing, travel, quarantine, and meet reporting requirements.

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

☒ Within the Bureau/Office:

Information may be shared with authorized human resources and occupational health and safety personnel who have a need to know to ensure effective implementation of the safety protocols, conduct workforce health and safety planning, oversee the program on status of employee vaccination, validate employee completion of certification forms, and to meet federal requirements.

☒ Other Bureaus/Offices:

Information may be shared with authorized bureau and office human resources personnel, occupational health and safety personnel, supervisors, and responsible officials who have a need to know to ensure effective implementation of the safety protocols and workforce health and safety planning, manage employee records on vaccination status, and meet federal requirements. Information may be shared with the Office of the Solicitor when necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement.

☒ Other Federal Agencies:

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 system of records notice, OPM/GOVT-10, Employee Medical File System Records, 75 FR 35099 (June 21, 2010); modification published at 80 FR 74815 (November 30, 2015).

☒ Tribal, State or Local Agencies:

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 system of records notice, OPM/GOVT-10, Employee Medical File System Records, 75 FR 35099 (June 21, 2010); modification published at 80 FR 74815 (November 30, 2015).

☒ Contractor:

Information may be shared with DOI contractors who are authorized to perform their duties for the Federal Government.

☒ Other Third-Party Sources:

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, 75 FR 35099 (June 21, 2010); modification published at 80 FR 74815 (November 30, 2015).

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

☒ Yes:

All DOI Federal employees must complete the form, however, providing information on their vaccination status is voluntary. Individuals are provided an opportunity to decide to provide their vaccination status or may decline to provide their status. A Privacy Act statement is provided on the certification of vaccination 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.

☐ No:

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

☒ Privacy Act Statement:

The Employee Certification of Vaccination form includes a Privacy Act statement.

☒ Privacy Notice:

Individuals are provided notice through the publication of this PIA and the OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), system of records notice.

☒ Other:

The Safer Federal Workforce Task Force web site provides comprehensive guidance to the public for the collection of vaccination status from Federal employees, as well as contractors and members of the public, the use of certification of vaccination forms, FAQs on safety protocols for individuals who are vaccinated, the legal authorities for collecting information, and privacy requirements for agencies to collect and maintain information on vaccination status from individuals under the Privacy Act and OPM regulations.

☐ None

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

Data may be retrieved by the employee's name, employee's email address, supervisor's name, supervisor's email address, or key word search.

I. Will reports be produced on individuals?

☒ Yes:

Reports may be developed by authorized human resources and health and safety officials on employee completion status for the form and vaccination status, which may identify individuals. Reports with aggregated metrics, such as the response rate of forms submitted, may also be produced. These reports 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. They must ensure that the sharing of those records are 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?

Information on employee vaccination status is collected directly from employees and is presumed to be accurate at the time of the employee's submission. The form requires that the employee attest to the accuracy and truthfulness of their responses before submission. Information on the employee's organization and supervisor may be verified with other DOI records to ensure complete and accurate records to support workforce health and safety planning and reporting.

In addition to the information collected from employees through the form, other information will be obtained from the Federal Personnel and Payroll System (FPPS) and other DOI human resources systems and merged with the data collected from individuals through the form for validation and reporting purposes, and to ensure data accuracy and quality. For example, existing DOI records will be used to verify the correct supervisor is identified in the employee records. This information includes the employee common identifier (ECI) (used in lieu of SSNs), assigned supervisor, bureau/office, sub-bureau/office organization, employee appointment type and status. DOI may also use records in DOI Talent and DOI Access to verify the employee and supervisor relationship to ensure only the correct supervisor has access to the assigned employees' information and protect employee privacy.

B. How will data be checked for completeness?

Information on employee vaccination status is collected directly from employees and is presumed to be complete at the time of submission. All fields in the automated form are mandatory, employees must complete all fields in order to submit the form. Human resources personnel will validate employee organization and supervisor through existing DOI records.

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

Information on employee vaccination status is collected directly from employees through a link to an automated form. The link remains valid to allow employees to update their status at any time by completing and submitting a new form. 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.

Employee medical files are maintained as occupations medical records pursuant to OPM regulations, 5 CFR Part 293, Subpart E, and Occupational Safety and Health regulations (29 CFR Part 1910.1020). An Occupational Medical Record is an occupation-related, chronological, cumulative record, regardless of the form or process by which it is maintained (e.g., paper document, microfiche, microfilm, or automatic data processing media), of information about health status developed on an employee, including personal and occupational health histories and

the opinions and written evaluations generated in the course of diagnosis and/or employment-related treatment/examination by medical health care professionals and technicians. This definition includes the definition of medical records at 29 CFR 1910.20(c)(6). Occupational Medical Records, as defined under OPM regulations, includes Employee Exposure Records and occupational illness, accident, and injury records.

Employee occupational medical records may be maintained in automated or paper form, and are located in approved locations within the agency. These records are part of a Governmentwide Privacy Act system of records established by OPM. As such, these records must be maintained pursuant to OPM Privacy Act regulations at 5 CFR part 297. Non-occupational/patient records pertaining to an employee may, under certain conditions, be maintained as occupationally related and may be included in the system.

These records are maintained in accordance with the National Archives and Records Administration General Records Schedule 2.7, Item 060, Occupational individual medical case files. The disposition is temporary. Short-term records are destroyed one year after employee separation or transfer (DAA-GRS-2017-0010-0010). Long-term records are destroyed 30 years after employee separation or when the employee's Official Personnel Folder 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?

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 information collected on employee vaccination status. The potential privacy risks identified include inadvertent or unauthorized disclosure, unauthorized access, use or alteration, lack of adequate notice,

collecting or using information that is not consistent with the purpose of the collection, collecting more information than is needed, and retaining information longer than necessary to support an authorized function. The risks are mitigated through security and privacy controls to protect the system and data in the employee medical files. The principle of least privilege is observed during all phases of the information lifecycle.

There is a risk that individuals may not receive adequate notice of the purpose of the collection or uses of their PII. This risk is mitigated by the Privacy Act statement provided on the Certification of Vaccination form, the publication of this PIA, and the OPM/GOVT-10 SORN. The OPM SORN provides instructions on how individuals may seek notification of, access to, or correction of their records in the system. The DOI Privacy Program website also provides guidance to individuals on how to submit a Privacy Act request or contact a privacy official for assistance or to submit a complaint. The Safer Federal Workforce Task Force website also contains comprehensive guidance on the use of the information collected in the form. Employees may voluntarily provide their vaccination status or may decline to provide their vaccination status on the Certification of Vaccination form and must follow the safety protocols in place for not fully vaccinated persons. Federal employees are advised that making a false statement on the Certification of Vaccination form could be subject to an adverse personnel action, up to and including removal from their position. It is also a federal crime (18 U.S.C. § 1001) for anyone to provide false information on the form. Falsification could also affect continuing eligibility for access to classified information or for employment in a national security position under applicable adjudicative guidelines. DOI does not request documentation to verify an employee's vaccination status. However, if DOI receives a good faith allegation that strongly suggests that an employee made a false statement on the Certification of Vaccination form, DOI may request documentation as part of its investigation into the alleged false statement. Employees may be subject to civil and criminal penalties as well as disciplinary action for making a false statement.

There is a risk of unauthorized access or disclosure of records or reports that contain PII, or that individuals may be able to view files or folders when access is mistakenly or unknowingly shared by the site owner, 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 of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015). 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 site owner and designated officials must take proper precautions when setting access permissions to ensure only those with a need to know are granted access. All data is stored and maintained in secure systems and is protected from unauthorized access by firewalls, intrusion detection systems, antivirus and the AD domain environment. User activity is monitored and logged to ensure only appropriate use of the system and data. To protect against unauthorized access, data is protected by strict access controls including two-factor authentication, least privilege principles and restricted access limited to authorized users. Authorized users and system administrators are required to complete annual Information Management and Technology (IMT) Awareness Training, which includes privacy and security

training, as well as role-based training to ensure they understand their responsibilities for safeguarding PII. Employees completing the form must also exercise caution and should take due care to prevent inadvertent or over-the-shoulder disclosures when entering responses.

There is a risk that the system may collect, store or share more information than necessary, the information may be used for an unauthorized 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 and will use replica data and other existing records to validate responses, enforce safety protocols and meet reporting requirements. 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 that records will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. This risk is mitigated by maintaining records in accordance with a NARA approved records schedule. 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 DOI Office of the Chief Information Officer (OCIO) provides management and oversight of Office 365, including system administration, security, enforcement of privileged users, authentication processes, and monitoring of the system. DOI uses Azure Active Directory Connect for user provisioning, identity management, and permissions management. DOI uses Active Directory Federation Services (ADFS) user authorization and authentication, which allows DOI to maintain control of user identification and authentication from within its network and operating environment. Additionally, access to all DOI systems including Microsoft Office 365 Cloud environment is Personal Identity Verification (PIV) credential enabled and configured to use multi-factor authentication. Access to this OneDrive file system where vaccination status information will be stored is restricted to the human resources and health and safety personnel on a need-to-know basis. The system owner is the site owner with authority and responsibility for establishing permissions to authorized users and managing access to the system records. Permissions may be established at different levels and are based on roles. Users will only see the information granted by the system owner. The system owner can also prevent edit access or downloads as necessary to ensure the confidentiality and integrity of the records.

Data in transit or at rest in Microsoft Office365 Cloud is encrypted. The Microsoft Office 365 Cloud system is integrated with DOIs Data Loss Prevention tools (DLP) tools to prevent manipulating files without authorization, printing protected data and exporting

protected/sensitive data outside a restricted file location. System auditing and logging takes place within the application to establish an audit trail of events.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The O365 is hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with Federal Information Security Modernization Act of 2014 (FISMA). The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and National Institute of Standards and Technology (NIST) guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information and is responsible for preventing unauthorized access to the system and protecting the data contained within the system. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels. The contract between DOI and O365 does not allow the service provider to review, audit, transmit, or store DOI data, which minimizes privacy risks from the vendor source.

Access controls are in place for HRIS-BI and SMIS. PII has been minimized where applicable prior to sharing data in HRIS-BI. HRIS-BI is used for the purpose of reporting statistical data on response rates to senior management. An individual's PII, including vaccination status is not provided in the report. Vaccination status data is not currently entered into SMIS, DOI's official accident and injury and illness reporting system. However, the SMIS PIA will be updated or a new PIA will be developed when the data is transferred into SMIS.

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:

☐ 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?

N/A

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.

Data is being consolidated from employee responses submitted through the certification of vaccination form and from existing human resources records in other DOI systems. This consolidation will help DOI ensure the most accurate information on the status of the employee and the relationship between employee and supervisor. Authorized officials need this information to manage the records, support efforts to implement safety protocols and ensure the health and safety of employees and meet reporting requirements.

☐ 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:

Access to data is determined based upon the user's role and position. Authorized users will only have access to the data that is required, based on their role, to perform their official duties. Departmental human resources personnel and health and safety personnel will have access to all the records in the system to perform their oversight, management and reporting duties. Bureau and office authorized personnel, managers, supervisors will only have access to records of the employees that are assigned to them.

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

Access to vaccination records will be restricted to the Office of Human Capital personnel on a need-to-know basis, and regularly reviewed by the ODfB site owner.

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.

The Office of Human Capital do not use contractors to support this system. Privacy clauses were inserted into the O365 contract.

☐ 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.

The O365 Security team general set of auditable events is specific to the O365 support and based on ongoing risk assessments of the system which incorporate identified vulnerabilities, business requirements, and O365 Security standards.

Audit capabilities include addition, modification, or deletion of data within the system. User activities are audited as part of the security monitoring controls to prevent any unauthorized monitoring or user behaviors. System logs capture username, date and time users access the system, changes that are initiated, and changes in user permissions.

☐ No

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

All user actions within the Microsoft O365 Cloud environment are logged. Audit logs are reviewed regularly and also when a significant change is made to the system to ensure any vulnerabilities exposed are being addressed by the set of auditable events. Auditable events include: event type; source; location; outcome; date/time and the entity associated with the event or user.

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

Security controls have been implemented to prevent unauthorized monitoring. Only authorized system administrators have access to audit logs. 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.

(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 Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect the employee medical files in the system in accordance with Federal laws, OPM regulations, OMB and Departmental policies. The System Manager is responsible for ensuring DOI meets requirements under the Privacy Act and OPM regulations and addressing any Privacy Act requests or complaints from individuals in consultation with DOI Privacy Officials.

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 Information System Owner and System Manager are responsible for oversight and management of the system and assuring proper use of the data in accordance with the Privacy Act, OPM regulations and DOI policy. All authorized users are responsible for immediately reporting any suspected loss, compromise, unauthorized access or disclosure of PII to DOI-CIRC, the Department's incident reporting portal, in accordance with the rules of behavior and the DOI Privacy Breach Response Plan.