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: U.S. Geological Survey - Financial Management and Security
Bureau/Office: U.S. Geological Survey/Office of Administration
Date: September 28, 2018
Point of Contact:
Name: Constance S. Sheffer
Title: Information System Security Officer
Email: ssheffer@usgs.gov
Phone: (703) 648-7433
Address: 12201 Sunrise Valley Dr., MS 159, Reston VA 20192

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The purpose of the U.S. Geological Survey (USGS) Financial Management and Security (FMS) system is to provide USGS project planning and budgeting, physical access control to the USGS National Center, and tracking of security clearances for USGS personnel. The FMS has the following components:

- Budget and Science Information System Plus (BASIS+)
  The purpose of BASIS+ is to provide USGS scientists and administrative officers with a tool for project planning and budgeting.

- Personnel Security and Clearance System (PSCS)
  The purpose of PSCS is to provide tracking of security clearances for USGS and Office of the Solicitor (SOL) employees.

- National Center Badging Information System (NCBIS)
  The purpose of NCBIS is to provide physical access control to the Reston, Virginia USGS facility for employees and tenants.

C. What is the legal authority?

Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulations); 5 U.S.C. 5514, 5701 et seq.; 26 U.S.C. 6402; 31 U.S.C. 3511 and 3512, 3701, 3702, 3711; 40 U.S.C. 483; Public Law 106-107, and 41 CFR 300-304.

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

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

010-000000988, 010-000001003; Systems Security Plan (SSP) for Financial Management and Security

☐No

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

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

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

☒Yes: *List Privacy Act SORN Identifier(s)*

DOI-45, HSPD-12: Identity Management System and Personnel Security Files, 72 FR 11036, March 12, 2007, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2007-03-12/pdf/E7-4407.pdf.

DOI-85, Payroll, Attendance, Retirement and Leave Records, 73 FR 19090, April 8, 2008, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2008-04-08/pdf/E8-7274.pdf.

☐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
☒Citizenship
☒Gender
☒Birth Date
☒Group Affiliation
☒Marital Status
☒Biometrics
☒Other Names Used
☒Truncated SSN
☐Legal Status
☒Place of Birth
☐Religious Preference
☒Security Clearance
☒Spouse Information
☒Financial Information
☒Medical Information
☒Disability Information
☒Credit Card Number
☐Law Enforcement
☒Education Information
☒Emergency Contact
☐Driver's License
☐Race/Ethnicity
☒Social Security Number (SSN)

☒Personal Cell Telephone Number
☐Tribal or Other ID Number
☒Personal Email Address
☐Mother’s Maiden Name
☒Home Telephone Number
☐Other: *Specify the PII collected.*

☒Child or Dependent Information
☒Employment Information
☐Military Status/Service
☒Mailing/Home 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*

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

☐Paper Format
☐Email
☒Face-to-Face Contact
☒Web site
☐Fax
☐Telephone Interview
☒Information Shared Between Systems
☒Other: *Describe* Data may be manually entered by authorized FMS personnel.

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

PII is used to conduct project planning, including budget reconciliation and salary projections, track HSPD-12 Personal Identity Verification (PIV) card applications for USGS affiliates and contractors, track security clearances for USGS employees, and control physical access to the USGS National Center in Reston, Virginia for employees and tenants.

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

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

Data are shared with USGS Human Resources offices when needed for hiring purposes regarding applicants that are converting to employees.

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

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

The HSPD-12 program is a government-wide requirement managed by the General Services Administration and is subject to Federal requirements for participating agencies that involve sharing of data - see government-wide system notice GSA/GOVT-7: Personal Identify Verification Identity Management System, for additional information sharing activities. Some information may be shared with other Federal Agencies as authorized pursuant to the routine uses contained in the DOI-45: “HSPD-12: Identity Management System and Personnel Security Files” and DOI-85: “Payroll, Attendance, Retirement and Leave Records” system of records notices.

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

Information may be shared with Tribal, state, or local agencies as authorized pursuant to the routine uses contained in the DOI-45: “HSPD-12: Identity Management System and Personnel Security Files” system of records notice.

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

Information may be shared with contractors who perform services or otherwise support DOI activities related to the FMS, and as authorized pursuant to the routine uses contained in the DOI-45: “HSPD-12: Identity Management System and Personnel Security Files” system of records notice.

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

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

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

Information is voluntarily provided by employees in order to obtain access to the USGS network and information systems, including those requiring security clearances. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the USGS network. If users decline to provide the required information upon employment at USGS they will not be given access to the network and may be unable to perform their duties.

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

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

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

The following Privacy Act Statement is provided to individuals filling out the SF-86 Questionnaire for National Security Positions:

Authority to Request this Information
Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Orders 10450, 10865, 12333, and 12968; sections 3301, 3302, and 9101 of title 5, United States Code (U.S.C.); sections 2165 and 2201 of title 42, U.S.C.; chapter 23 of title 50 U.S.C.; and parts 2, 5, 731, 732, and 736 of title 5, Code of Federal Regulations (CFR).

Your Social Security Number (SSN) is needed to identify records unique to you. Although disclosure of your SSN is not mandatory, failure to disclose your SSN may prevent or delay the processing of your background investigation. The authority for soliciting and verifying your SSN is Executive Order 9397.

☐Privacy Notice: *Describe each applicable format.*

☐Other: *Describe each applicable format.*

☐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 are retrieved by any defined field within the record. These fields include, but are not limited to: name, organization code, or social security number.

I. Will reports be produced on individuals?

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

Reports include project salary projections by individual, used to track expenditures and balance budgets. Project managers can only view their staff, but regional managers have access to regional data. Reports are also provided to the Office of Personnel Management (OPM) in order for OPM to track and manage the background investigation requirements and maintain assigned security clearance levels.

☐No

Section 3. Attributes of System Data

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

Data manually collected from individuals are verified for accuracy during OPM's background investigation.

B. How will data be checked for completeness?

New data go into suspended status until FMS staff can review and screen for completeness.

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

Data are updated nightly. As new records are added, they are marked as suspended until verified by FMS staff.

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

Data are retained in accordance with the corresponding USGS General Records Disposition Schedule (GRDS). The applicable GRDS include 701-05a: Budget Reports, where data are destroyed after seven years; 903-01: Security Clearance and Access Authorization Administrative Subject Files, where data are destroyed after three years; and 903-04a: Contractor HSPD-12 Credentialing Files, where data are destroyed no later than 5 years after employee separation or notification of death, whichever is earlier.

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

Paper records are shredded or pulped in accordance with records retention guidelines. Electronic records are deleted. Backup tapes are reinitialized and reused. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy, and National Archives and Records Administration guidelines.

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 privacy risk to individuals due to the limited information contained in the FMS system and the mitigating controls implemented to protect data. FMS authorized end users are allowed to edit or view the documents based on their authorized subsystem roles and the specific job functions. System, network, application, and database level access is controlled strictly on a need-to-know basis. Appropriate background investigations are conducted before any access is granted. No anonymous access is allowed. All system activities are logged and constantly monitored. All employees and contractors with access to the system must go through an annual IT security awareness and privacy awareness training. Appropriate warning banners are displayed at the login time. All system users must acknowledge and follow the rules of behavior as prescribed in the system rules of behavior.

FMS 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) standards. FMS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII contained in the system. The FMS has developed a System Security Plan based on NIST guidance and is part of a Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on the FMS to identify and mitigate any found. Security and privacy awareness training is required for all USGS employees and information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter, and sign the DOI Rules of Behavior. Security role-based training is also required for security personnel and officials with special roles and privileges.

USGS complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Access to administrative functions is strictly controlled. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource.

Section 4. PIA Risk Review

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

☒Yes: *Explanation*

Data captures project work plans, project budgets, and account and funding information. It allows users to build project budgets, narratives, and goals into a project plan with query and reporting capabilities for standard and ad-hoc reports. It provides summary and management reports that are used to track project budget status as well as work progress and accomplishments. Data in FMS also enables the USGS to monitor and report on both active and inactive security clearances, and pinpoint recertification and security briefing needs for USGS and SOL employees. It also monitors HSPD-12 PIV card issuance, activity, and terminations for affiliates and contractors.

☐No

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

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

☒No

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

☐Yes: *Explanation*

☒No

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

☐Yes: *Explanation*

☒No

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

Not Applicable. FMS does not use electronic collection to derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

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

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

☒No, data or processes are not being consolidated.

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

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

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

Role Based Access Control is used to implement least privilege access to data. Mangers can only see data for their employees. Regional staff can access to regional data via their assigned role. Roles are described in the Access Control Standard Operating Procedures document.

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

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

☐No

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

☐Yes. *Explanation*

☒No

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

☒Yes. *Explanation*

Audit logs are used to record access to the system, and access to the data. Logon date and time, IP address, logoff data and time and process accessed are recorded in system audit logs. Database logs are used to track transactions by users. Logs are reviewed daily.

☐No

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

IP Address, Logon and Logoff time and processes accessed are recorded in Audit Log Files.

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

USGS complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any FMS equipment. The use of USGS IT systems is conducted in accordance with the appropriate use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator’s identification); and activities that could modify, bypass, or negate the system’s security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Access to administrative functions is strictly controlled. Additionally, users must be included in security groups assigned to a resource in order to access that particular resource. Also, all users must complete IT security and privacy awareness training, as well as role based training on an annual basis and before being granted access, and sign 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. *Describe*

(3) Administrative Controls. Indicate all that apply.

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

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

The FMS System Owner serves as the Information System Owner and the official responsible for oversight and management of FMS's security and privacy controls, including the protection of information processed and stored by FMS. The Information System Owner and the FMS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by FMS. The System Manager is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the USGS Privacy Officer.

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 FMS Information System Owner is responsible for oversight and management of the FMS security and privacy controls and for ensuring, to the greatest possible extent, that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team immediately upon discovery in accordance with Federal policy and established procedures.