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: Administrative Financial System (AFS)
Bureau/Office: National Park Service – Accounting Operations Center
Date: October 28, 2021
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, 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 Administrative Financial System (AFS) is a web-based system for financial tracking, reporting, budget formulation, budget execution, and executive level reporting. AFS is used in more than 500 parks and offices throughout the National Park Service (NPS). AFS increases the

speed and efficiency of decision-making within the NPS. AFS is comprised of roughly 250 Forms and Reports. Customers depend on AFS to perform their daily mission across the NPS.

AFS is a custom developed reporting application using commercially available development tools that resides on the internal NPS network and is not available to the internet or public facing. Data for AFS is extracted from the Financial and Business Management System (FBMS) and delivered to AFS via secure file transfer protocol using the DOI Secure Transport system. AFS uploads and deletes the data file transfer daily, and AFS users can then add non-PII information such as notes and descriptions to the uploaded FBMS records for operational purposes.

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:
UII: 010-000000480, Administrative Financial System 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.*
None			

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

☐ Yes
☒ No

Records in FBMS are maintained under DOI system of records notices including: DOI–86, Accounts Receivable: FBMS – July 28, 2008, 73 FR 43772
DOI–87, Acquisition of Goods and Services: FBMS – July 28, 2008, 73 FR 43766
DOI–88, Travel Management Records: FBMS – July 28, 2008, 73 FR 43769
DOI–89, Grants and Cooperative Agreements: FBMS – July 28, 2008, 73 FR 43775

AFS contains labor hours/costs associated to NPS employees and this information is used by the Bureau's budget office for the purpose of financial planning. The records within AFS are covered under INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records, July 19, 2018, 83 FR 34156. The DOI-85 SORN can be viewed at https://www.doi.gov/privacy/sorn.

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
☒ Financial Information
☒ Other:

The Employee Common Identifier (ECI) assigned by the Federal Personnel and Payroll System (FPPS) and employee hours worked are used to compare actuals to budgeted amounts for labor categories.

Name, User id and password, nps.gov email address are used for account management purposes.

The FBMS assigned Vendor Number is used to associate information to a business entity. The vendor number may identify officers of the business entity, including sole proprietorships which may be linkable to an individual.

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:

Data for AFS is extracted from the FBMS and delivered to AFS via secure file transfer protocol using the DOI Secure Transport system. Information is collected via secure file transfer from the FBMS, and the FBMS Privacy Impact Assessment is available at: https://www.doi.gov/sites/doi.gov/files/uploads/fbms_cloud_pia_final_0.pdf

DOI Secure Transport is a web-based Transport Layer Security (TLS1.2 enforced) file transfer system that allows authorized users the ability to securely transfer files between DOI users, bureaus and offices, and internal or external customers either manually or via system scripted uploads and downloads. The Privacy Impact Assessment for Secure Transport is available at: https://www.doi.gov/sites/doi.gov/files/uploads/secure-transport-st-pia-final-04212020.pdf

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

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

Data for AFS is extracted from the FBMS and delivered to AFS via secure file transfer protocol using the DOI Secure Transport system.

For DOI users, information for account management is collected from the individual during onboarding or generated as DOI records (e.g. email address, User Principal Name (UPN), username) during operational activities. To establish an account for a DOI user, an authorized NPS manager emails (encrypted) a user account request to the system administrator. The system

administrator creates the user account with the information provided, and the queries the Active Directory Federated Services to validate and complete the account creation.

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

Vendor and employee information including vendor number, ECI, name and employee hours worked, are used to compare actuals to budgeted amounts for labor categories.

PII collected from users for account management will be used to securely authenticate individuals to the system, manage user roles and permissions, and enable change and audit logging.

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

☒ Within the Bureau/Office:

AFS data is available to all administrative offices for those users that have the appropriate roles within the NPS for the purposes of budget planning.

☐ Other Bureaus/Offices

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☒ Contractor:.

NPS may contract with other commercial organizations to provide application development, configuration and operations, and maintenance of AFS or specific subsystems. Contractor staff will be required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need to know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system.

☐ Other Third-Party Sources

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

☐ Yes

☒ No:

For data imported from FBMS, consent for collection of data is address in the FBMS Privacy Impact Assessments, and AFS reporting is consistent with uses identified in the FBMS Privacy Impact Assessments.

For NPS Users information is collected from the individual during onboarding or generated as DOI records (e.g. work email address, UPN, username) during operational activities at the individual park sites by park staff. PII is collected from NPS Users who must use the system to perform the duties of their employee, contract or volunteer position.

NPS Users consent to provide information during the onboarding process. NPS Users may decline to provide information during the onboarding process; however, this may result in reassignment to another position or a withdrawal of the offer of employment or opportunity to volunteer, with that determination made at the park or other level where the user will be performing his or her duties.

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

☐ Privacy Act Statement

☒ Privacy Notice:

Privacy notice is provided through publication of this privacy impact assessment and applicable SORNs.

☐ 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.).

Reports may be generated from name, ECI, business area, organization identifier, pay period, or vendor number to retrieve labor related information.

I. Will reports be produced on individuals?

☒ Yes:

Labor Reporting Report identifies labor costs by pay periods, business areas and organizations, or fund areas and programs. The reports can drill down to detailed labor cost record information

needed to verify individual employee labor charges by account assignment. For instance, the system can generate detail reports by business area, employee, pay period, to report the number of hours recorded by pay code and account assignment. A Labor Interface Specialist may extract reports to ensure proper classification and reconciliation of labor charges.

Account management reports are produced on NPS Users and are reviewed and analyzed weekly for inappropriate or unusual privileged and non-privileged user activity. Reports in the form of audit logs may include name, action such as "Access Requested", action details, application, role, access level, requestor, approver and approver role. Reports are used for auditing and system access tracking.

☐ No

Section 3. Attributes of System Data

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

All PII data except account management is collected from NPS/DOI records, and this data cannot be edited. Only non-PII information, such as notes and descriptions, can be appended to the NPS/DOI records, and NPS employees and supervisors are responsible for verifying the accuracy of the information.

Prior to secure file transfer upload, AFS conducts audit procedures daily for the file transfer to ensure the accuracy and completeness against records counts and totals to ensure the consistency between the file sent by FBMS and the file received by AFS.

For NPS users, information is collected from the individual during onboarding or generated by NPS or DOI as DOI records (e.g. email address, UPN, first name and last name) during operational activities.

B. How will data be checked for completeness?

All PII data except account management is collected from NPS/DOI records, and this data cannot be edited. Only non-PII information, such as notes and descriptions, can be appended to the NPS/DOI records, and NPS employees and supervisors are responsible for verifying the completeness of the information.

Prior to secure file transfer upload, AFS conducts audit procedures daily for the file transfer to ensure the accuracy and completeness against records counts and totals to ensure the consistency between the file sent by FBMS and the file received by AFS.

DOI users are responsible for ensuring the completeness of the data associated with their user accounts and content posted in the system. PII used for account creation is initially provided by

the individual during onboarding. During the account creation process, the user account administrator will validate the account request against DOI Active Directory information, and incomplete data will result in an error preventing creation of the account. Incorrect data may prevent user authentication or may be identified by supervisors when reviewing activity reports. Users may contact the help desk for assistance to validate account information and follow published procedures to have the data updated.

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

AFS has audit procedures to ensure the file transfer is received and executed daily to ensure data is current and remains consistent with FBMS.

Employees and supervisors are responsible for ensuring account management information is current in AFS. Users may contact the help desk for assistance to validate account information and follow published procedures to have the data updated.

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

Records are retained in accordance with the National Park Service Records Schedule, Management and Accountability (Item 10), which has been approved by the National Archives and Records Administration (Job No. Nl-79-08-9). The disposition for routine fiscal, contracting, and purchasing records is temporary and records are destroy/delete 7 years after closure. The disposition for routine housekeeping and supporting records is temporary and records are destroy/delete 3 years after closure.

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

Records are disposed of in accordance with the applicable records schedule and Departmental policy. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 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.

The privacy risks to individuals is considered moderate due to the PII collected and is mitigated by the limited PII maintained in the system, name, official contact information, labor codes, work orders. ECIs are used in lieu of Social Security numbers to mitigate risk to the privacy of individuals. AFS is categorized as a moderate risk system; however, multiple controls have been implemented to mitigate and substantially lower privacy risks. All information acquisition and collection is done through electronic web forms over encrypted communication channels

that comply with the required federal standards and stored within an encrypted database to minimize risk of data breaches while in transit and while stored. Information access and retrieval is done through electronic web forms over encrypted channels following defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS data center policy and process for backup and retention of information. A formal Assessment and Authorization for issuance of an authority to operate is being conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system is rated as moderate, requiring management, operational, and technical controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. As part of continuous monitoring, continual auditing will occur to identify and respond to potential impacts to PII information.

There are privacy risks related to hosting, processing and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which are referenced in the System Security and Privacy Plans. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties.

Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

The risk of data interception in transit is mitigated through encryption. Data is protected in transit from FBMS to AFS by SFTP. AFS authenticates to the FBMS server using public key infrastructure (PKI). Both AFS and FBMS use SSH host key fingerprints for verification/non-repudiation when establishing the connection. Data is protected in transit between the AFS web server and the end user by TLS.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees and contractors are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing users to access and update only their records in the system. For DOI user accounts, this risk is further mitigated by validating information against DOI Active Directory, authentication results, and activity report and audit log content. No sensitive PII is collected or managed by the system.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that information including PII may be output from AFS to physical media and improperly secured or disposed. All PII information including reports is access-controlled, and only NPS staff with the appropriate need-to-know will be given access. DOI mandates that all Federal employees and contractors complete initial and annual information security and privacy training. The resulting high awareness provides an enhanced level of assurance on the life cycle management of the PII data. Physical media including printed reports is manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards until the physical media is disposed of by shredding or pulping for paper media or erasing or degaussing for electronic physical media.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA and the applicable SORNs.

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: ECI, name, vendor number, organization id and employee hours worked are necessary to compare actuals to budgeted amounts for labor categories.

☐ 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?

The system does not derive or create new data.

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: *Describe*

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

AFS accounts are provisioned by the regional coordinators or security managers. After approval from the regional AFS coordinators, AFS security managers, or the government system owner (depending on access requested). This access control list is maintained in AFS. AFS data is

restricted vertically by role as well as horizontally by organization or office. AFS roles are assigned based on the principle of least privilege.

Access is restricted for all users. Each user will be assigned a role (functions) and permissions. The role will determine what function the user may execute in the system while the permissions will define what records the user can create, read, edit or delete. Select PII data fields will be encrypted and only available on a need to know basis.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee or contractor staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

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 responsible for designing, developing and maintaining the system, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

Contractor employees interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. Information security and role-based security training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to sensitive data; however, no sensitive PII is collected or managed by the system.

☐ 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

Monitoring will primarily target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

☐ No

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

AFS is not intended for monitoring users, however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including identity verification method, action attempted and the status of the attempt, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

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

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

Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any AFS assets. Only authorized users with valid DOI Active Directory credentials will be able to access the AFS system. In addition, all users must consent to Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training before being granted access to the DOI network or any DOI system, and annually thereafter.

AFS users are presented with the following Terms and Conditions of Use prior to signing on to the application:

Terms and Conditions of Use

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems

may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system.

Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

(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 Deputy Manager, Management Systems serves as the AFS Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in AFS. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within AFS, in consultation with NPS and 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 AFS Information System Owner and Chief of AFS are responsible for oversight and management of the AFS security and privacy controls, and for ensuring to the greatest possible extent that AFS data is properly managed and that all access to data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI Computer Incident Response Center and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.