

**U.S. Department of the Interior**  
US Geological Survey  
Office of Administration and Enterprise  
Information

---

Financial Management and Security System  
FMS

**Privacy Impact Assessment**  
May 2014



---

Prepared for the Department of the Interior  
1849 C Street, NW, Washington, DC 20240

---

**Department of the Interior  
US Geological Survey  
Privacy Impact Assessment**

**Name of Project:** Financial Management and Security System (FMS)

**Bureau:** US Geological Survey (USGS)

**Office:** Administration and Enterprise Information (AEI)

**Project's Unique ID:** 010-12-01-01-03-2002-00-402-124

**A. CONTACT INFORMATION:**

Name: William P. Reilly  
Title: IT Specialist, USGS APS  
Address: USGS National Center, 12201 Sunrise Valley Drive, MS 802  
City/State/Zip: Reston, VA 20192  
Phone: 703-648-7239  
Fax: 703-648-7229  
Email: [wreilly@usgs.gov](mailto:wreilly@usgs.gov)

**B. SYSTEM APPLICATION/GENERAL INFORMATION:**

1) **Does this system contain any information about individuals?**

**a. Is this information identifiable to the individual<sup>1</sup>? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).**

Yes.

<sup>1</sup> "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- b. Is the information about individual members of the public? (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).**

Yes

- c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).**

Yes.

**What is the purpose of the system/application?**

The Financial Management and Security System (FMS) system is a collection of financial management and security applications used by USGS employees to process various financial transactions and/or report related financial information for science projects. Only authorized USGS users' with valid system accounts and appropriate access privileges can access this system from the Intranet or via the USGS approved remote access technology from the Internet. No anonymous access is allowed. All communication channels are appropriately encrypted and all system activities are constantly monitored. The servers that host these applications reside inside the USGS managed network infrastructure that follows the defense-in-depth security best-practices, and all applicable USGS security policies, guidelines, and procedures.

The following subsystems comprise the FMS system:

- Personal Security and Clearance System (PSCS) - This subsystem enables the USGS Security Office to track and report on security clearances for the USGS employees and contractors, and is used for designating those employees who need a security clearance recertification or security briefing.
- National Center Badging and Information System (NCBIS) - This subsystem is used to secure access to office and data center areas at the National Center. It helps maintain records of the individuals entering and exiting the National Center controlled areas via the use of the Identocard 9000 access control system (i.e. ingress and egress times).
- Integrated Business Solutions (IBiS) - The IBiS system supports the Science Information Delivery Office in the distribution of all USGS published materials such as: maps, books, and scientific reports. Other federal agencies such as the National Park Service (NPS), Bureau of Land Management (BLM), Forest Service (FS), The National Map (TNM), and National Imagery Mapping Agency provide products that are also distributed from the IBiS system. The IBiS customer base is comprised of internal USGS, Federal and non-Federal government, Business Partners, and the General Public,

- Budget and Science Information System Plus (BASIS+) - This subsystem is an enterprise wide web-enabled system that is used to capture the 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. The system operates in conjunction with other systems that establish and maintain official accounting and personnel records. These include the FBMS and the Federal Personnel and Payroll System (FPPS). It also provides the operating budgets information to the FBMS. It also uses the expenditure transactions information from the FBMS for the management reporting purpose. The BASIS Plus uses the information from the FPPS and the USGS Lotus Notes Name and Address Book for the employee reference data verification purpose.

**3) What legal authority authorizes the purchase or development of this system/application?**

OMB Circular A-127	<i>Financial Management Systems</i>
Public Law 97-255	<i>Federal Managers' Financial Integrity Act</i>
Public Law 101-576	<i>Chief Financial Officers Act of 1990</i>

### **C. DATA in the SYSTEM:**

**1) What categories of individuals are covered in the system?**

Internal USGS, Federal and non-Federal government, Business Partners, and the General Public.

**2) What are the sources of the information in the system?**

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Depending upon the specific subsystem functionality used, either an individual end user inputs his/her own information or inputs the information about the other USGS employees, contractors, or partners. The general public provides information for IBiS.

**b. What Federal agencies are providing data for use in the system?**

Department of the Interior and USGS are the only agencies providing data for use in this system.

**c. What Tribal, State and local agencies are providing data for use in the system?**

No Tribal, State or local agencies are providing data for use in the system.

**d. From what other third party sources will data be collected?**

No data will be collected from the third party sources. The data will be collected from the Department of the Interior or USGS managed systems.

**e. What information will be collected from the employee and the public?**

Information is normally collected directly from an authorized end user or from an authorized official reference resource in the USGS/DOI. BASIS+ and PSCS contain employee information and SSN. SSN is not a visible field in the BASIS+ application. Contact information (name, street address, city, state, zip code, and credit card information) is provided by the general public for the purchase of maps, National Park Passes, publications and books.

**3) Accuracy, Timeliness, and Reliability**

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

Not Applicable. There is no data being collected from other sources other than DOI records.

**b. How will data be checked for completeness?**

End users are normally expected to check, verify, and certify the accuracy and completeness of all the data they submit. BASIS+ has built-in features to check and validate the input data for formatting and completeness.

**c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

Yes, the data is kept current via timely data input and regular automated data replication processes.

**d. Are the data elements described in detail and documented? If yes, what is the name of the document?**

The specific data elements are appropriately documented within each of the subsystem design, development, test, and operations support documents as per the USGS standard policy and practices.

**D. ATTRIBUTES OF THE DATA:**

**1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes. The data that is being captured via the FMS subsystems is relevant and necessary for the mission and services rendered by the USGS. Earlier, these data elements used to be captured via various paper based forms. The new standards and workflow based subsystems help streamline the USGS business and administrative processes, and helps in increasing the efficiency, effectiveness, and business reputation of the USGS organization.

**2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No, the FMS system does not derive new data or create previously unavailable data through aggregation. Various subsystem specific data is actually stored and managed in separate databases.

**3) Will the new data be placed in the individual's record?**

Not applicable as no new data is created.

**4) Can the system make determinations about employees/public that would not be possible without the new data?**

No, the system cannot make determinations about employees or the public that would not be possible otherwise. No new data elements are created by this system.

**5) How will the new data be verified for relevance and accuracy?**

Not applicable as no new data is created.

**6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Not applicable. Data is not being consolidated within this system.

**7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Processes are not being consolidated within this system. The 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.

**8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Depending upon the specific subsystem or database, data can be retrieved via various means such as an employee name or phone number, invoice number, vendor identification number, etc.

**9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Depending upon the specific subsystem database, various types of reports can be produced as required to support the bureau mission or business process need. Examples would be the summary of funds report for a specific project or the journal voucher audit report.

**10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Personnel are made aware of their right to view/access or change their personal information on some of these databases in accordance with USGS DOI 319-1-H, Guide for Handling Privacy Act Records; and the Privacy Act of 1974, as amended, (5 U.S.C. 552a). DOI Privacy Orientation and Awareness online training course is also available. However, for all Financial Management System related forms the use of the social security number is mandatory for all the USGS employees and vendors it is used to process electronic payment of invoices, track security clearances or to generate the BASIS+ funds reports that are used to manage funds.

**E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:**

**1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The FMS system is maintained at the USGS site in Reston, Virginia. USGS general ledger is maintained at the Denver site and the subsidiary ledger information is maintained at the Reston site. IBiS executes at the Denver Federal Center.

**2) What are the retention periods of data in this system?**

FMS data retention period will be in accordance with the USGS General Records Disposition Schedule (GRDS 432-1-SI).

**3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Procedure is to destroy/delete when dissemination, revision, or updating is completed. Disposition procedures for this data will be in accordance with the USGS General Records Disposition Schedule (GRDS 432-1-S1).

**4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

The system is not using the technologies that DOI or the bureaus have not previously employed.

**5) How does the use of this technology affect public/employee privacy?**

The contents of some of the subsystems data contain the Privacy Act sensitive information. Access to the actual subsystem data is limited to a small group of authorized individuals who have a need-to-know based limited access. No anonymous access is allowed, and system data is not accessible to any unauthorized personnel.

**6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Based on the specific information available in some of the subsystems, the identity and location of the USGS employees, contractors or partners can be identified. This actually helps in expediting the approval and business processing. All activities of all the individuals using this system- can be appropriately logged and monitored by the authorized officials. All end users are warned at the login time that there no right to privacy in this system.

**7) What kinds of information are collected as a function of the monitoring of individuals?**

All success and failure activities related to the account logon and logout, all account management activities, audit policy change, system events, session initiation, use of privileged commands, forms approval and disapproval, etc. are recorded. All failure activities such as the object access, use of privileged commands, access attempts to system and data files, etc. are also recorded. All users are warned at login time that no right of privacy exists when using this system and all of their activities may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel.

**8) What controls will be used to prevent unauthorized monitoring?**

Collected data is well protected in accordance with the established Privacy Act procedures, and by a combination of user id, password, and access control list(s). Only a very small group of authorized personnel have a need-to-know based limited access to the system data. Limited numbers of authorized users have privileged access to various systems, monitoring tools, devices, or management reports. DOI Privacy Orientation training is provided to all system users. No Anonymous access is allowed. All privileged system and database access activities are appropriately recorded and monitored. All users are required to go through an annual IT security awareness and privacy awareness training. All users are expected to follow the rules of behavior for the system.

**9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

FMS system operates under the following DOI Department wide System of Record Notices (SORN) and USGS SORNs:

- Interior/DOI-58, Employee Administrative Records, Interior
- Interior, DOI-86 Accounts Receivable: FBMS
- INTERIOR/USGS-23, Personnel Investigations Records
- INTERIOR/USGS-27 Office of Management Services (OMS) Badging and Access Control System

**10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

If the scope of the personal data maintained in the FMS system is modified, the appropriate System of Records will be modified or a new one will be created as is necessary for the operation of the system.

**F. ACCESS TO DATA:**

**1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

USGS employees or contractors who have an active valid login account and system role will have need-to-know based limited access to the system information resources and data.

**2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to data by user is determined by his or her approved role assigned in the system access profile. Depending upon the business process need and the sensitivity of the specific subsystem data elements, need-to-know based granular access control lists are applied at the system, network, application, and database field level to limit the system users' access to the appropriate data elements and functionality.

**3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

Authorized users access to the system data is restricted based on his or her specific role.

**4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Rules of Behavior documented in the System Security Plan (SSP) controls the misuse of data by those having access. In addition, the FISSA+ online training course emphasizes the need to respect and ensure the privacy of system data. Data access is controlled using established roles within each asset.

**5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes. Contractors involved in the design, development, maintenance or operation of the system are required to go through the same type of background investigation check and privacy training that the Government employees go through. Same rules of behavior govern the contractors and the government employees. The USGS IT Statement of Work is required for all IT related purchases.

**6) Do other systems share data or have access to the data in the system? If yes, explain.**

The BASIS+ subsystem is a subsidiary financial management system and shares some of its data with the FBMS. Expenditure data is downloaded nightly into BASIS+ and project data is uploaded into FBMS nightly. IBiS has a nightly upload to FBMS for financial data.

**7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Everyone who has authorized access to the system, including the System Owner, Information Systems Security Officer, Chief Information Officer, and the Privacy Act Officer is responsible for protecting the privacy rights of public and employees affected by this system. Currently, electronic files are not shared with any other automated applications.

**8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

No other agencies will share or have any direct access to the data maintained in this system. However, DOI FBMS will share or report some of its financial data with the Department of Treasury as required by various business process need, statutes, and laws.

**9) How will the data be used by the other agency?**

FMS data files are currently not directly shared with any other external agency.

**10) Who is responsible for assuring proper use of the data?**

Everyone who has authorized access to the system, including the System Owner, Information Systems Security Officer, Chief Information Officer, and the Privacy Act Officer is responsible for assuring the proper use of the data.

