

Department of the Interior
Privacy Impact Assessment

September, 13, 2010

Name of Project: Financial Business Management Systems
Bureau: Office of the Secretary (OS)
Project's Unique ID (Exhibit 300): 010-00-01-01-01-1127-24

A. CONTACT INFORMATION:

NBC Privacy Officer
1849 C Street NW, Mailstop MIB-2650
Washington, DC 20240
Phone: 202-219-8526

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any information about individuals** *{this question is applicable to the system and any minor applications covered under this system}?*

Yes, FBMS contains privacy-related information about individuals.

- a. Is this information identifiable to the individual**¹ *{this question is applicable to the system and any minor applications covered under this system}?* (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F can be marked not applicable. If YES complete all sections for system and any applicable minor applications).

Yes, the information as described above is characterized as personally identifiable information.

- b. Is the information about individual members of the public** *{this question is applicable to the system and any minor applications covered under this system}?* (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes, the information as described above pertains to individuals that can be members of the public and/or employees.

- c. Is the information about employees** *{this question is applicable to the system and any minor applications covered under this system}?* (If yes and there is no information about

¹ "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).

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, the information as described above pertains to individuals that can be members of the public and/or employees.

2) What is the purpose of the system/application?

The FBMS Major Application (MA) addresses the challenge of maintaining disparate, bureau-level financial and business management processes through consolidation using a uniform set of processes that are standardized across all bureaus and offices within the Department. The FBMS MA solution, when fully implemented, will be used by over 70% of DOI employees; it will affect all employees and operations. As such, this project involves all parts of the department, as well as all Departmental Strategic Initiatives and the President's Management Agenda. FBMS system components will be interfaced to departmental, bureau-specific, and external systems in order to support the DOI Business Process Operations. The FBMS MA solution, when fully deployed, will meet the following DOI objectives:

- Implement a department-wide solution that will standardize and integrate financial and business management processes while meeting all applicable current and future security and privacy requirements.
- Provide business intelligence and analytic capabilities to financial and business management processes to strengthen decision-making capabilities and reporting that will enable executives, managers, and other employees to more effectively carry out the department's missions.
- Ensure financial and business management data and transactions are recorded properly, accurately, timely, and efficiently with strong internal controls.
- Satisfy critical and routine internal and external requests for financial and business management related information and data.
- Provide a solution that economically and efficiently leverages technology over the solution's life cycle and accommodates changes in Federal laws, regulations, and financial and business management mandates.
- Implement, reform, and streamline key financial and business management processes, building on available government and industry best practices to improve performance and reduce operating costs.
- Provide a solution that fosters employee retention, professionalism, creativity, and excellence and implements cultural transformation within DOI's financial and business management communities.
- Implement an effective document and records management solution for financial and business management activities that meets standard records management requirements.
- Enable an effective migration from the legacy environment to the new financial and business management solution through available risk minimization techniques.
- Provide a solution with the capability to balance financial and business management workload across DOI.

2a) List all minor applications that are hosted on this system and covered under this privacy impact assessment:

There are no minor applications that are hosted on this system.

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

FBMS is authorized to operate by various financial statutory and regulatory provisions, including 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.

C. DATA IN THE SYSTEM:

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

FBMS supports on-line transaction processing by external grant applicants and DOI employees. The users of the Core Financials and Acquisitions functionality of FBMS are Bureau of Land Management (BLM), Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) and Office of Surface Mining (OSM) Bureau employees. The users of the Financial Assistance functionality are external citizens and foreign nationals as well as BLM, BOEMRE and OSM bureau employees. The users of FBMS are currently:

- BLM, BOEMRE and OSM bureaus
- External citizens who are grant applicants or grantees for programs offered by BLM, BOEMRE and OSM.

For the upcoming Deployment 5 (D5) of FBMS, scheduled for November, 2010, employees of an additional bureau, the United States Geological Survey (USGS) will be added to the FBMS user base.

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?

Data stored in FBMS will always enter through:

1. Initial data conversions from legacy systems into FBMS
2. Ongoing individual user interaction with the FBMS system
3. Ongoing interfaces from non-FBMS systems into FBMS

Regardless of the data entry method, the data will always be subject to the same set of business rules and validity checks enforced by the underlying FBMS software.

These three sources of data entry are described in detail below.

1. Initial Data Conversions

As bureaus implement FBMS, and their legacy financial, grant and acquisition systems are retired, a wide variety of data may be converted into FBMS including: assets, funds, cost centers, work breakdown structures, accounting code derivation tables, vendor and customer master data, requisitions, purchase orders, invoices, reimbursable agreements, contracts, travel advances and obligations, fleet data, property, equipment, work orders, and maintenance plans, data and tasks.

Often incoming data must be scrubbed and cleaned, as the underlying SAP Enterprise software enforces stringent data integrity and referential checks. Thus a major task during bureau implementation is to perform dry runs of legacy data conversions and clean data that does not pass the required validations and referential integrity checks.

As an example, one source of data for the current Core Financials component of FBMS was the data residing in the BOEMRE and OSM ABACIS applications, which were the legacy bureau financial systems replaced by FBMS. This data was converted into FBMS during several dry runs and then for real during the Final Cutover Conversion activities.

The primary source of data for the Financial Assistance FBMS application component was the grant data from the BOEMRE and OSM Bureaus. This data was converted into FBMS during the initial go-live phase of the FBMS project in February 2005.

2. Ongoing Individual User Data Entry

FBMS users can perform a wide variety of business functions in the following general business areas:

- Core Financials
 - Manage Accounts Payable
 - Manage Accounts Receivable
 - Perform Funds Management
 - Process Asset Transactions
 - Process Reimbursable Transactions
 - Process Grants Transactions
 - Process Charge Card Transactions
 - Process Labor Cost Distribution Transactions
 - Perform Project Planning and Project Accounting
 - Perform General Ledger Accounting
 - Perform Cost Allocation/Perform Activity Based Costing
 - Perform Internal and External Auditing
 - Use OpenText LiveLink (IXOS) for Source Documents
- Financial Assistance
 - Create Notice of Funding Availability
 - Create and Post Announcements to Grants.gov
 - Approve Award Recommendations and Commit Funding
 - Obligate Funding and Award Financial Assistance
 - Manage the Award (amendments, status, audit, site visits, etc.)
 - Close Financial Assistance Award
- Acquisitions
 - Conduct Advanced Procurement Planning
 - Prepare Purchase Requisitions
 - Conduct Market Research
 - Develop Requirements
 - Solicit Quotations/Formal Sealed Bids/Proposals
 - Order Goods & Services
 - Administer Contracts & Orders
 - Receive, Inspect, & Accept Goods & Services
 - Process Payments & Contract Closeout
 - Maintain Suppliers
- Enterprise Management Information; Business Warehouse reporting on:
 - GL/SPL Line Items
 - AP Line Items
 - AR Line Items
 - SD - Sales & Billing Line Items
 - FM – Budget, Commitment & Actual Line Items
 - CO – Cost & Allocation Line Items
 - PS – WBS Line Items
 - Charge Card – Data & Hierarchy
 - Labor – Employee Master Data & Labor Cost Data
 - Hyperion – Acquisition – Purchasing Data
 - FA – R/3 Data

Deployment 3, implemented 11/2007, introduced the acquisition component for BOEMRE and OSM to the FBMS solution, supported by FBMS components PRISM, SAP ERP 2005 and SAP Business Warehouse. The conversion activities for acquisition included

gathering and associating acquisition data from the bureau legacy IDEAS systems into the FBMS system.

Deployment 4, implemented 12/2008, added an additional bureau to the FBMS user base – the Bureau of Land Management (BLM). The deployment added functionality in the areas of Personal Property Management, Fleet (Vehicle) Management, and interfaces to the new travel management system – eGov Travel.

Deployment 5, scheduled for 11/8/2010, will add an additional bureau to the FBMS user base – the United States Geological Survey (USGS).

Deployment 5 will also add additional functionality in the area of Real Property.

3. Ongoing Interfaces to External Systems

The external systems that FBMS interfaces with can be grouped into one of the following four categories:

1. DOI Departmental Level Systems
 - ABC/M System
 - FPPS
 - Hyperion
2. DOI Bureau Specific Systems
 - FEEBACS
 - Collection and Billing System
 - Alaska Fire Store
 - National Interagency Fire Center
 - Office of Aircraft Services (OAS)
 - Basis Plus+
 - Maximo
 - IBIS
 - Standard Revenue
3. Non-DOI Systems – Government
 - FedBizOpps
 - Grants.Gov
 - CCR
 - GSA
 - Treasury
4. Non-DOI Systems – Non-Government
 - Smart Pay Charge Card
 - E-Gov Travel
 - Fed-Connect

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

The following Federal agencies provide data to FBMS and the interfaces are discussed in section 2.a.3 above:

- BLM
- GSA
- BOEMRE
- OSM
- Treasury
- USGS

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

For Deployment 5, there are no tribal, state or local agencies providing data for use in the system.

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

All of the following sources of data are covered in section 2.a above.

1. DOI Departmental Level Systems
2. DOI Bureau Specific Systems
3. Non-DOI Systems – Government
4. Non-DOI Systems – Non-Government

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

FBMS contains privacy-related information about individuals. It is important to note that a significant portion of the information contained in the FBMS system will not be about individuals; however, some information, as identified in the bulleted list below, will relate to individuals.

The information provided below addresses concerns of privacy-related information as an aggregate, meaning that not all of the information provided in the list below is necessarily privacy-related by itself. However, when the information provided below is directly associated with data that is classified as “sensitive” or “privacy-related,” then the data related would be reclassified to a higher sensitivity level.

- Grantee reported expenditures information used to obligate grant funding which includes grantee name, vendor/DUNS number, address, and bank account number.
 - It is possible that some grantee information may use a social security number in place of a vendor/DUNS number. An example would be an individual that is applying for a grant who uses a social security number because they do not have a vendor/DUNS number. In this example, the associated contract may then use the social security number provided in place of a tax identification number such as a vendor/DUNS number.
- Employee names will be part of AP vendor master files if an employee has received an AP check (travel advances and vouchers). Data elements may include employee name, employee number, social security number, address, and bank account number.
- Employee charge card information will be received via an interface from the credit card provider, and maintained in FBMS to support the reconciliation of expense vouchers.
- Basic employee master file information is updated in the FBMS application via interface from the Federal Personnel and Payroll System (FPPS). Employee information is required in FBMS for processing of travel and relocation vouchers as well as certain labor cost postings. Employee level data is required for Labor Adjustments, but the vendor number is used to identify the individual. Since the vendor number is associated with a name and amount, it is still sensitive.

Vendor identifiable data may include vendor name, vendor number, address, and bank account number.

3) Accuracy, Timeliness, and Reliability

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

Data integrity checks will be performed by FBMS as incoming and outgoing data is processed through the FBMS portal. Both systems will contain data integrity checks to ensure data accuracy. Data that conforms to business rule and integrity checks will be posted. Non-

conforming data will be posted to a suspense file for examination and resubmission upon correction.

b. How will data be checked for completeness?

Data will be checked for completeness as it is entered into the system. DOI-defined business rules and database integrity will determine if the data is complete. One type of verification of completeness check involved creating a list of valid inputs and checking inputs against the table.

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).

Data is checked to see if it is current and not duplicated by comparing the incoming data with the data already in the system. This check is performed when being processed through the FBMS portal.

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

The core FBMS project documentation is constantly under review and updated with each release of FBMS. All project documentation regarding data elements resides in the Rational ClearCase database.

The underlying SAP ERP and SAP BW systems at the heart of FBMS maintain metadata (documentation of the data elements) within various system tables within the FBMS application itself. Thus, the FBMS production system has available integrated data dictionary and data element browsers.

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.

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, FBMS does not create or derive new data about an individual.

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

Not applicable for FBMS deployment 5. (No new data).

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

Not applicable for FBMS deployment 5. (No new data).

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

Not applicable for FBMS deployment 5. (No new data).

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

Layers of Control for Data in the FBMS systems:

- Data will be categorized by Bureau/office and many other levels discovered via the blueprint stage. Functional team designs end user roles and restrictions from Bureau level down to document type level.
- The application security team generates roles using authorization objects to grant access by whatever level necessary via the requirements gathered by the technical team and the subject matter experts (SMEs). Roles are designed to only give view of system transactions to the level the defined roles are assigned. SMEs associated with the FBMS security procedures will be made up of DOI employees and those familiar with the FBMS processes, security role development and functionality. In addition, SMEs test roles against live data during multiple testing cycles.
- All end users will be categorized by their parent Bureau, (i.e., BOEMRE, Bureau of Land Management). Bureaus will assign a Bureau security point of contact (SPOC) to work with the FBMS security team to refine/define authority roles.
- Bureau SPOCs (BSPOCs) will activate, update and deactivate Bureau Accounts for their respective Bureau accounts. The BSPOC is granted authority to assign end user roles for their respective Bureau. The bureau level approval authority will be twofold and include both the end user's supervisor approval for FBMS accounts and the Account Controller(s) approval for role assignment.
- Central SPOCs (CSPOCs) will activate, update and deactivate accounts for all NBC, the Project Team and all central Master Data Maintenance (MDM) roles. The CSPOCs can activate NBC/IT/security, FBMS project team, and BSPOC accounts, meaning that they can create accounts with default roles only. The CSPOC is granted authority to assign central and default roles. The approval authority for MDM accounts will include the end user's supervisor and the NBC finance management team. The approval authority for the FBMS project team and all SPOC roles will be the FBMS Information System Security Officer (ISSO).
- The Elevated Access SPOCs (ESPOCs) will be used for elevated access management for all FBMS users. ESPOCs can assign elevated access roles to all FBMS users (i.e. assign roles only). The ESPOC is granted authority to assign only elevated access roles for configuration, developer, technical, advanced functional, and SPOC Roles. The approval authority for the ESPOCs will be the FBMS ISSO.
- All role additions/change requests by the SPOCs will be recorded and kept for future audit purposes.
- Root system user IDs are secured with strong passwords that change on a regular cycle. The use of the root system user ID accounts is limited in the production environment, requiring project manager's approval. The security team will monitor the root user IDs and password, as well as requests, on the behalf of the Basis team.
- System end user accounts will be monitored for use on a regular basis. All accounts inactive for 90 days are locked.
- Password requirements follow the standards of OS/NBC per the DOI IT Security Policy Handbook

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

All data will conform to a naming convention for each Bureau/office. All end-users will be restricted by the naming conventions. Bureau leads or their designee will approve access for the end-users, in addition to a scheduled review of assignments to users IDs. The Bureaus

will have the authority to approve data access from role development to approvals for role assignment. The applications have the ability to restrict at the finest level, including data at the field level.

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.

Yes, a personal identifier is used to retrieve data. The identifiers are listed below:

- Applicant Information
 - Employee ID number (EIN)
 - DUNS number
 - Applicant name (company name or person)
 - Street address
 - Organization ID
- Applicant Project Director Information
 - Name
 - Phone
 - Fax
 - Email
- Vendor Information
 - Vendor number
 - Name
 - Social Security Number (only for DOI employees carried within the vendor file to support travel voucher reimbursement payments)
- Charge Card Information
 - Last name
 - First name
 - Account number

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

Financial Assistance Reports

- **Applications**
 - **Preapplication**

The Preapplication Report provides a printed version of the data that is displayed on the Preapplication form. The layout of the report is similar to that of the SF-424 fact sheet. This report also prints narratives. The word "Draft" will be displayed on the top of the report until the preapplication has been submitted.

Applicants (have access to only their data), financial assistance administrators, financial assistance staff, staff reviewers, peer reviewers, and award approvers will have access to this report.
 - **SF-424 Application**

The SF-424 Application provides a printed version of the SF-424 application, narratives, the work plan, project plan, or objectives worksheet, the required documents checklist, and a list of all subapplications, as applicable. The word "Draft" will be displayed on the top of the report until the application has been submitted to the Agency or to the prime applicant.

Applicants (have access to only their data), financial assistance administrators,

financial assistance staff, staff reviewers, peer reviewers, and award approvers will have access to this report.

- **Budget Cover Sheet**

The application budget cover sheet summarizes the application's budget by budget category, displays subtotals for each section and totals for the entire budget, and displays the percentage shares for the Agency and the grantee.

Applicants (have access to only their data), financial assistance administrators, financial assistance staff, staff reviewers, peer reviewers, and award approvers will have access to this report.

- **Budget Narrative**

The budget narrative shows the detailed budget line item information for all budget items. Applicants (have access to only their data), financial assistance administrators, financial assistance staff, staff reviewers, peer reviewers, and award approvers will have access to this report.

- **Reviews**

- **Announcement Information**

The Announcement Information Report lists detailed information about an announcement including the title, announcement type, modification number, dates, Agency information and award information. The report can be printed in either PDF format or XML format. This format is selected on the Announcement Information form. The Notice of Funding Availability (NOFA) administrator, financial assistance administrators, and financial assistance staff will have access to this report.

- **Review Administration**

- **Detailed Pool Report**

The Detailed Pool Report provides detailed information on the reviewers available to participate in peer reviews for the specified NOFA. The information includes reviewer demographics, comments, and prior experience. Financial assistance administrators will have access to this report.

- **Peer Reviewers**

The Peer Reviewers Report provides information about the reviewers who have been confirmed for a peer review for the specified NOFA. This includes the review dates, reviewer contact information, and special accommodations required by a reviewer, if any. Financial assistance administrators will have access to this report.

- **Contact Information Report**

The Contact Information Report lists all reviewers in a peer review pool for a NOFA with their phone numbers, e-mail addresses, and whether the reviewers have been contacted, accepted, confirmed, and participated. Financial assistance administrators will have access to this report.

- **Group Travel Order**

The Group Travel Order report lists the travel-related information about reviewers selected for a Peer review for applications submitted under the specified NOFA. Costs are broken down to include airfare, per diem expenses, lodging and the honorarium paid to non-Federal employees.

Financial assistance administrators will have access to this report.

- **Miscellaneous Obligations for Peer Review**

The Miscellaneous Obligations for Peer Review lists the travel related information about reviewers selected for a Peer review under the specified NOFA. This includes information such as honorarium, miscellaneous obligation number and accounting code. Financial assistance administrators will have access to this report.
- **Review Reports**
 - **Reviewer Worksheet**

The Reviewer Worksheet lists the applications reviewed by a reviewer, ranked with the score assigned to each application by the reviewer. It also lists the scores and the reviewer comments for each scoring category under an application. It can be run for one or all reviewers under a NOFA. Financial assistance administrators and award reviewers will have access to this report.
 - **Consensus Worksheet**

The Consensus Worksheet lists the applications submitted under a specified NOFA ranked by the consensus score assigned by a panel. It also lists the reviewers in the panel for each application, along with their comments. Financial assistance administrators and award reviewers will have access to this report.
 - **Consensus Report**

The Consensus Report lists the applications submitted under a specified NOFA ranked by the consensus score assigned by a panel. It also lists the consensus comments for each scoring category under an application. Financial assistance administrators and award reviewers will have access to this report.
 - **Review Panels Consensus Summary**

The Review Panels Consensus Summary report summarizes the applications under a NOFA, including the applicant organization and program names, the state in which a program will be located, and the peer review stage 1 and 2 scores and ranks. Financial assistance administrators and award reviewers will have access to this report.
 - **Applicant List for a NOFA**

The Applicant list for a NOFA report lists the names of the applicant organizations, the proposed FTEs, budgets, and sites for each applicant, and totals for the NOFA. Financial assistance administrators and award reviewers will have access to this report.
 - **Review Recommendations**

The Recommendation Summary report is available for prime applications that include subapplications. The report lists all of the subapplicants with their requested budgets, full time equivalents (FTEs), status, and includes the recommendation summary entered by the prime applicant regarding each subapplication. Financial assistance administrators and award reviewers will have access to this report.
 - **Application Summary**

The Application Summary report summarizes the applications assigned to the specified NOFA, and includes the service categories addressed by each application. Financial assistance administrators will have access to this report.
 - **Applications Dropped after Peer Review**

The Applications Dropped after Peer Review report lists the applications that have not recommended for funding, including the application organization's name, the

state the organization is from, whether the organization has applied for Agency grants before, and the rank on the peer review panels that evaluated the application. This may include applications that are still being reviewed. Financial assistance administrators and award reviewers will have access to this report.

- **Application Status Report**

The Application Status report lists all applications under a NOFA by their current status. Financial assistance administrators and award reviewers will have access to this report.

- **Competitive New and Re-compete Recommendations**

The Competitive New and Re-compete Recommendations report lists the staff recommendations for applications, grouped by region, under the specified NOFA. It includes information such as the funding level, number of FTE positions, and the legislated area. It also includes the change in the funding level and number FTE positions between the present year and the previous year. For the funding level and the number of FTE positions, it lists the values requested by the applicant and the values recommended. Financial assistance administrators and award reviewers will have access to this report.

- **Review Process Evaluations**

The Review Process Evaluations report prints the evaluations entered by reviewers and facilitators. Financial assistance administrators will have access to this report.

- **Correspondence**

- **Letters and emails**

Letters can be printed and emails sent from the Correspondence module. Financial assistance administrators will have access to this report.

- **Grant Awards**

- **Notice of Grant Award**

The Notice of Grant Award (NGA) is the document that constitutes the legal agreement between the grantee and the Agency for funding the grantee's project. An email is sent to the grantee when the award is made. The grantee can then log on to the financial assistance process to view/print the NGA. Only the most recently awarded NGA for a grant can be printed. Grantees can only view/print NGAs for their own organization. Financial assistance administrators and award recipients will have access to this report.

- **Financial Status Report**

The Financial Status Report is a printed version of the SF-269 report based on the entries made in the database. Financial assistance administrators and award recipients will have access to this report.

Labor Reporting Report

- **Business Warehouse**

Reports can be generated from the FBMS Business Warehouse that identify 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.

Charge Card Reports

- **Business Warehouse**
 - **Charge Card Restricted Role**

Access is granted to an Agency/Organization Program Coordinator (AOPC) to create management control reports. These reports may assist in tracking budget, supporting 1099 processing, and supporting program controls for card settings and defaulting schemes.
 - **Customer Master Restricted Role**

General Customer Query – Restricted

Acquisitions, Contracting Officers, Contracting Officers Technical Representatives and Receiving officials may have general vendor query access in order to verify DUNS, Taxpayer Identification Number and CCR data. Also, Core Finance Systems Accountants and Master Data Maintenance personnel may have general customer master query access in order to verify address, payment terms, ALC, and DUNS.
 - **Vendor Master Restricted Role**

General Vendor Query – Restricted

Financial Assistance Grants Officers, Senior Grants Officers, Program Officers, and NOFA Administrator's may have general vendor query access in order to verify DUNS, Taxpayer Identification Number and Recipient ID.
 - **Deployment 2 History Restricted Role**

PayTrans History Query - Restricted

Financial Assistance Grants Officers, Senior Grants Officers, Program Officers, Budget Officer's, and NOFA Administrator's may have access to BOEMRE payment history via the following two roles:

Payroll History Query (Restricted for BOEMRE bureau personnel only)

Tran50 History Query (Restricted for BOEMRE bureau personnel only)

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.)

Not applicable for FBMS. PII is transferred to FBMS via system interfaces and individuals do not provide PII to FBMS.

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 system is not operated in more than one site. All production components, with the exception of DOI Active Directory (AD) servers, are located in the NBC hosting center.

While there is only one instance of the "FBMS system," there are multiple environments supporting the production environment of FBMS. That is, there are also development, testing

and training environments supporting the production environment within the “FBMS system” landscape. PII in the non-production environments is secured as follows:

1. Through strict network access controls access to the FBMS non-production environments is restricted to a limited number of DOI users, primarily the FBMS Support Team and Bureau Subject Matter Experts (SMEs).
2. The FBMS non-production environments are not accessible to the Internet.
3. Access to the FBMS non-production environments is controlled using user name and password authentication.
4. The PII is scrubbed in non-production environments where there is not a business requirement to maintain the data.

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

The retention period for the data will vary, depending on the type of document or data. Data will only be removed by users that have access rights to remove content from the system and are familiar with established retention requirements (see below).

Data will be maintained in accordance with applicable Records Schedules, NARA and Departmental guidance. FBMS is currently being reviewed by the OS/NBC Records Office to determine appropriate records retention and disposition instructions. Until such a time as an approved records schedule is created or verified to exist, the data within FBMS is considered unscheduled, and thus Permanent.

2b) 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?

There are currently no procedures for disposition of the data, as a retention period has not been established. Reports will be kept in accordance with their new record classification (default is 1204 N1-048-08-22 for Routine Reports; individual reports must be assessed by subject matter experts).

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

No new technology is being implemented.

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

N/A

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

No

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

N/A

7) What controls will be used to prevent unauthorized monitoring?

Controls outlined in the FBMS System Security Plan that adhere to the standards outlined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, are in

place to prevent unauthorized monitoring. This includes the use of role-based security, encryption, and maintaining data in secured facilities, among others. It is important to note that FBMS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

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

Records on individuals maintained within the FBMS are covered by the following four Privacy Act Systems of Records Notices (SORNs), reviewed and approved by the DOI Solicitor, Office of the CIO, Executive Secretary, and Security Information Officer. These SORNs have been published in the Federal Register and can found at the following URLs:

Interior, DOI-86: Financial and Business Management System (FBMS) – Accounts Receivable
<http://edocket.access.gpo.gov/2008/E8-17250.htm>

Interior, DOI-87: Financial and Business Management System (FBMS) – Acquisition of Goods and Services
<http://edocket.access.gpo.gov/2008/E8-17248.htm>

Interior, DOI-88: Financial and Business Management System (FBMS) – Travel Management Records
<http://edocket.access.gpo.gov/2008/E8-17249.htm>

Interior, DOI-89: Financial and Business Management System (FBMS) – Grants and Cooperative Agreements
<http://edocket.access.gpo.gov/2008/E8-17264.htm>

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

The SORNs for DOI-86 and DOI-88 were existing notices that were revised and republished for FBMS in the Federal Register on July 28, 2008. The revisions were due to the implementation of FBMS.

The SORNs for DOI-87 and DOI-89 are new notices that were published for the first time in the Federal Register on July 28, 2008. The notices were created due to the implementation of FBMS.

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)

The system administrators will have access to a production client that is void of configuration and data. The developer will not have access to the production client that contains transactional data. This will not change, unless circumstances require a person to get approval for access to the data.

The contractors/functional team will have display rights on the production instance only, minus data deemed sensitive.

Users and managers will first be limited to the Bureau then on an as-needed basis as defined and determined by job functions.

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

FBMS follows Governmental and Departmental standards for application access controls. All system access requires user name and password authentication. The FBMS Access Control Policy outlines the requirements for gaining access to FBMS.

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

At the department level some may have access to all of the data on the system. This is being determined through business requirements definition.

At the bureau level the users will have all display access minus items that are deemed sensitive. Specific roles will be created to address detailed access control initiatives.

3) 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)

It is the responsibility of the Bureau Account Controller's (ACs) to determine proper accesses for their users. It is also the ACs duty to periodically recertify their users for proper assignments. For separation of duties purposes, the ACs are only allowed to assign end user roles. An independent process is in place to provide other accounts that have elevated access.

All users will be trained on the functions that they will be performing before Go Live. Auditing is also performed to monitor user activity.

All equipment containing sensitive or privacy related data has undergone the standard hardening as documented by approved Security Technical Implementation Guides (STIG) configuration guidelines.

FBMS leverages the ESN as the single remote access solution. This provides limited access points to the system from remote locations. The ESN Remote Access Solution has a session timeout set at 30 minutes for inactivity. In addition, the ESN is monitored 24/7/365 by personnel trained to report incidents involving sensitive and/or privacy-related information. These individuals work out of the DOI's Network Operations and Security Center (NOSC).

4) 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?

Contractors are designing and developing the system and will be involved with the maintenance. Contractors undergo a background check and sign non-disclosure agreements, as per DOI procedure and guidance. Privacy Act contract clauses were inserted in their contracts and other regulatory measures has been addressed.

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

Yes, the Labor Interface IFF070 transmits external payment amounts to the FPPS HR System hosted by NBC. External Payment Amounts (Pay Code 66A) are defined as any amounts not directly reimbursed to the employee, including items such as centrally billed items on the employee's Integrated Charge Card, Third Party Payments obligated on a RM-triggered Obligation as well as payments made to a Relocation Services Company (RSC). Bi-weekly, according to the Payroll Schedule, extracted data from R/3 is uploaded to FPPS.

Maintenance is performed on this table via an R/3 Maintenance Screen. Maintenance of the table is performed by the bureau's Labor Interface Administrator.

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

The FBMS team and the SPOCs will be responsible for protecting privacy rights.

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

No.

8) How will the data be used by the other agency?

Not applicable for FBMS Deployment 5. There is no sharing of data with other agencies

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

Not applicable for FBMS Deployment 5. There is no sharing of data with other agencies