Privacy Impact Assessment for FMS-NG

A. Data in the System

1. Generally describe the information to be used in the system.

The Financial Management System-Next Generation (FMS-NG) is a custom configured Commercial off the Shelf (COTS) solution, which supports flexible financial accounting, control and disbursement of funds, management accounting, and financial report processes. More specifically, the FMS-NG maintains the Ex-Im Bank's spending budget, supports buying of goods and services, outgoing payments for goods and services, records general ledger entries, reports to Department of Treasury and the Office of Management and Budget (OMB), verifies data accuracy, properly clears and closes ledgers and journals, and provides complete loan and guarantee servicing over the entire life of credit.

FMS-NG is comprised of the following functional modules:

- budget execution,
- accounts payable,
- accounts receivable,
- general ledger,
- purchasing, and
- processing of loans and guarantees financial data

The FMS-NG system data contains Personally Identifiable Information (PII) on Ex-Im Bank customers, employees, contractors, business partners (providers of goods or services). The system also collects PII on invitational travelers who have been asked to speak at or attend a function at the request of Ex-Im Bank and who are seeking reimbursements for expenses incurred. The PII information is stored encrypted in place and https protocol is employed in accessing FMS-NG.

The identifying data for individuals, such as their name and residential address information, may be linked in the FMS-NG system to
1) the individual's Social Security Number (SSN),
2) the individual's banking information - bank account numbers and the American Bankers Association (ABA) routing numbers for wire transfers and Automated Clearing House (ACH) payments, or
3) both the SSN and the Banking information. Table 1, enumerates the PII Data Elements in FMS-NG.

Table 1. Representative PII Data Elements within FMS-NG

PII Data Elements
ACCOUNT_HOLDER_NAME
ACCTTYPEID

PII Data Elements
ADDRESSID
BANK_ACCOUNT_NAME
BANKACCOUNTID
BANKSWIFTCODE
BRANCHID
BRANCHNAME
CHECK_DIGITS
PARENT_VENDOR_ID
PARENT_VENDOR_NAME
TAX_ID
VENDOR_ID
VENDOR_NAME
VENDOR_NAME_ALT
VENDOR_NUMBER

2. What are the sources of the information in the system?

Information contained in the FMS-NG is obtained using one of three methods: manual entry, direct database connection to supply the required information, and through consumption of source flat files imported using PLSQL procedural upload to the FMS-NG database. There are seven distinct sources of information for FMS-NG:

1) Manual data entry by the Office of the Chief Financial Officer (OCFO) staff of the approved annual administrative budget for the Bank, broken down by specific funding codes and fiscal year. The Bank's budget figures are entered into the FMS-NG budget execution module and subsequently maintained by the OCFO staff.

2) Manual data entry by non-OCFO Ex-Im Bank employees and invitational travelers of the personal financial information in order to obtain reimbursement for approved travel expenses incurred by the individual. Individuals seeking reimbursement voluntarily disclose their full name, American Bankers Association (ABA) Routing Number, and Account Number for the financial institution where they wish the Ex-Im Bank to send direct deposit reimbursements.

3) Ex-Im Bank-operated Comprizon Suite electronic procurement system, is the source of the purchase order detail describing the funding agreements and contracts issued to a supplier to which the Bank creates an obligation to pay. Purchase orders and award documentation are prepared by the Office of Contracting Services staff using the Comprizon Suite software. FMS-NG does not connect directly to the Central Contractor Register (CCR)/System for Award Management (SAM) database for information; all identifying data originating in CCR is supplied to FMS-NG by the Comprizon Suite.

4) Fedwire Collections Information Repository (CIR) system supplies the information about sponsored travel, insurance policy premiums and shipment payments. That information is obtained by file extracts from Fedwire CIR database.

5) Ex-Im Bank-operated Application Processing System (APS) supplies the authorization and participant information associated with `new and updated bank financial products, such as long-term loan and guarantee, and working capital guarantee commitments. Applications for these products originate from a variety of the Bank's customers including suppliers, borrowers, obligors, lessees and lessors, guarantors and buyers. Their applications are serviced solely within APS. FMS-NG consumes only a subset of applicant information, pertaining specifically to the financial obligations of the Bank from the point of obligation through final disbursement/payment, write-off, or claim/rescheduled debt servicing creation.

6) Ex-Im Bank-operated Ex-Im Online (EOL) system is the source of the authorization, insurance premium payment, shipment reporting, broker commission payment and participant information associated with new and updated medium-term loan and guarantee, and insurance commitments. Applications for these products come from a variety of customers including exporters, suppliers, brokers, borrowers, obligors, lessees and lessors, guarantors and buyers and are serviced within EOL. FMS-NG consumes only a subset of that information pertaining specifically to the financial obligations of the Bank from the obligation through final disbursement/payment. Information contained in the Master Data Management (MDM) tool is consumed by FMS-NG system via EOL. There is no direct interface from FMS-NG to MDM.

a. What Ex-Im Bank files and databases are used?

No Ex-Im Bank generated flat data files are used as source data for FMS-NG.

Two Ex-Im Bank databases are used:
(1) The EXIMPROD server database, supporting Comprizon Suite, Application Processing System (APS) and Ex-Im Online (EOL) is hosted at Ex-Im Bank Headquarters;
(2) The FMSPROD server database, supporting FMS-NG. FMSPROD is a cloud-based configuration hosted at Oracle's Managed Cloud Services' (MCS) facility in Austin, Texas.

b. What Federal Agencies are providing data for use in the system?
FMS-NG receives flat files from the Department of Treasury. These files include the data from the Fedwire CIR database and the Intra-Governmental Payment and Collection (IPAC) database.

c. What State and Local Agencies are providing data for use in the system?
None

d. What other third party sources will data will be collected from?
None

What information will be collected from the Ex-Im product applicants, contracted suppliers or individuals?

FMS-NG will contain customer information related to the financial obligations of the Bank from the point of obligation through the point of final disbursement/payment and provides complete loan and guarantee servicing over the entire life of credit. Customer data (See Table 1, Enumeration of PII Data Collected) would include: customer name, the name of the "Care Of" entity, U.S. address (street, city, state, and zip code), foreign address, and foreign contact name and for the cash control functions - bank account information for wire transfers/Automated Clearing House (ACH) payment. Analogous information will be collected for any contracted suppliers doing business with Ex-Im Bank Corporate Name, Corporate Address, Phone Number, Dun & Bradstreet (D&B) Data Universal Numbering System (DUNS) identifier number, Employer Identification Number (EIN), and banking account and banking routing number for wire transfers/ACH payment. In some cases sole proprietors of business use their individual SSN in place of EIN. In these cases SSN number will be collected.

The FMS-NG system will contain Personally Identifiable Information (PII) on Ex-Im Bank employees and public individuals that incurred expenses pre-authorized for reimbursement, Ex-Im product applicants, and contracted suppliers. The PII data being collected includes Name, Address, Phone Number, SSN, and Bank account and ABA routing number for wire transfers/ACH payment.

3. How is integrity of the data assured?

a. How will data collected from sources other than Ex-Im Bank records and the exporter be verified for accuracy?

The accuracy of the individual and business records is verified by the individuals at the time of data entry. The entries may be subsequently updated as needed.

Specifically, PII information is voluntarily disclosed by Ex-Im Bank employees seeking reimbursement of the authorized expenses by entering it in the 'Authorization for Direct Deposit' form. It is the employees' responsibility to ensure that the financial information they provide is accurate and up to date. The same applies to invitational travelers who are seeking reimbursements for the pre-authorized expenses incurred while speaking at or attending a function at the request of Ex-Im Bank. It is the individual's responsibility to ensure that the financial information they provide for the purpose of receiving a direct deposit reimbursement is accurate.

Identifying information supplied to FMS-NG by the Comprizon Suite originates in the CCR database. That information is initially entered and subsequently maintained in the CCR database by the business entities themselves. Its accuracy is dependent on the entities in a business relationship with the Bank.

b. How will data be checked for completeness?

Completeness of the data is primarily checked by the individuals and business representatives submitting the data. The individuals are also responsible for subsequent maintenance and update of their records. The FMS-NG application enforces field validation of select fields to

preclude manual entry of incomplete or nonsensical data or omission of data entry in the mandatory fields.

Specifically, the CCR registrant's data (supplied to FMS-NG by the Comprizon Suite) is originally entered by the registrant and can be modified by the registrant at any time. The identifying information stored in the FMS-NG Oracle database for the application is continually refreshed through routine downloads from CCR to Comprizon Suite. Employee financial information used for reimbursements via Direct Deposit is disclosed and updated by each employee and submitted to OCFO Cash Control staff for entry. OCFO staff is responsible for making the entries to update this information as needed.
All manually entered FMS-NG data is checked for completeness by the OCFO staff during data entry.

Select data fields contained in FMS-NG, for example, zip codes and SSN/EIN numbers, have been implemented to enforce the entry of valid characters and values within the specified range limits. The implementation precludes the entry on nonsensical data, such as letters instead of numbers, and provides cross-checks of the field information from other authoritative sources. FMS-NG performs consistency tests and other validations to ensure that the data in these fields is complete and accurate. The relevant PII fields have been implemented to check the completeness of data entered into each screen, such that no mandatory fields are left blank.

c. Is the data current? How do you know?
The currency of the FMS-NG data is based on the FMS-NG interfaces and data entered manually by the user. Applicants for Bank services submit information that provides the current state of their organization and export financing requirements at the time of submission of each application. Such data is maintained in the APS, EOL and MDM applications. This data is updated at renewal time or as a result of a D&B match. Each applicant attests to the currency, completeness, and accuracy of the data submitted with their applications at the time of submission. The applicable subset of the data from other systems is loaded into FMS-NG via system interface upon authorization.

For business entities that deliver products or services to the Bank and Bank employees, current information on each individual or business is maintained in the Comprizon Suite application. The business partner files in Comprizon Suite are maintained via secure transfer from the CCR database to Comprizon. Every private business entity (including the sole-proprietorships) that conducts business with the Federal Government is required to enter and maintain its corporate information on the SAM website and is solely responsible for the currency, completeness, and accuracy of the data they submit.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
FMS-NG is a configured Oracle Federal Financials Release 12. Oracle Federal Financials COTS is a collection of Oracle E-Business Suite modules and functionality used by U.S. Federal Government Agencies. The data elements are documented in the FMS-NG Oracle Federal

Financials system views and the system documents enumerated in Table 2, FMS-NG Data Elements Documentation List.

Table 2. FMS-NG Data Elements Documentation List.

FMS-NG Documents
F&A Data Model
ACH check format SPS Outbound Interface Design_Draftv0.1.docx
Comprizon Interface Design Draft v0.2.docx
EOL Insurance Inbound Interface Design_Draftv0.3.docx
EXO-LGA GTE Interface Design.xls
Fedwire Collection to AR Inbound Interface Design_Draftv0.1.docx
FMS-NG FA Data Model and Mapping 071713.docx
LGA Agreement Attributes.xlsx
LGA_GL_Information.xlsx
Loan_Inbound_Data_Mapping.xlsx
MDMCustomerDataMapping.xlx
Purchase Order Inbound Interface Design_Draftv0.2.docx
Sponsored Travel Inbound Interface Design.docx

B. Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?
The list of FMS-NG user classifications and access rights is consistent with the existing Ex-Im Bank's Financial and Administrative (F&A) systems and Administrative Accounting Activities (AAA) system user access rights. The list encompasses the following Ex-Im Bank business categories roles: Budget (Manger Role and User Role); Payables (Manger Role and User Role); Purchasing (Manger Role and User Role); General Ledger (Manager Role and User Role); CRM Resource Manager Role; Credit Administration User Role; Functional Manager Role; HRMS Manager Role; Loan Guarantee Servicing User Role; Portfolio Manager Role; Receivables User Role ; and a System Administrator Role.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?
FMS-NG has configurable Responsibilities-based (processes and data) user access rules. The users with specific access privileges are enumerated and documented in the user-role mapping tables for FMS-NG. Primary access to the FMS-NG data is via the FMS-NG Oracle Federal Financials. A robust three-step user authentication procedure is built into accessing FMS-NG.

- Step one: the user must authenticate to the Bank's internal Local Area Network.
- Step two: the user signs into FMS-NG and is authenticated using the FMS-NG Oracle COTS login. All users must be authenticated prior to being granted FMS-NG system access.
- Step three: user access within FMS-NG is configured using the system authorization scheme (with respect to FMS-NG responsibilities, role, and data-based access).

Authorized users may also access certain FMS-NG data elements downloaded to Exim's data warehouse via Ex-Im Bank Reporting System (ERS), an Oracle Business Intelligence application, and Oracle Enterprise Performance Management (EPM) (formerly Hyperion). These Oracle tools are accessible to authorized internal users only. The use of ERS and EPM for accessing FMS-NG data is in the read-only mode.

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

FMS-NG users will have restricted access only to the data subset necessary to perform their job function. This access is managed via Oracle Applications System Administration, User and Responsibility security functions.

The Bank employs COTS software tools capable of both "canned" queries (pre-specified set of data, generated for a pre-configured report within the dashboard functionality) and ad hoc queries that are constructed at access time. Both Oracle's EPM tool and ERS possess the capability for the canned and ad hoc queries. These Oracle based-tools are accessible by authorized internal users only and are used in read-only mode. No data contained in FMS-NG may be changed by the users of these tools. Access to EPM and ERS is managed via access control systems built into each of them. ERS also employs role-based security to ensure that authorized users see only the data authorized by the business unit of the respective user.

Finally, the entire Bank's staff (employees and contractors) must complete a background check - National Agency Check with Inquires (NACI) as a condition of employment at the Bank. Each employee completes mandatory annual training in IT security awareness and government employee ethics, which includes training in handling of PII data. Senior employees are required to submit an annual financial disclosure form. All contractors are annually required to complete the Bank's IT security awareness training and to sign a Non-Disclosure Agreement (NDA). As such, the Bank's staff is considered to be "trusted insiders," knowledgeable about the Bank's policies and procedures, with an understanding that authorized access to the Bank's IT systems cannot be used for unauthorized purposes.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

FMS-NG has controls on both processes (Responsibilities) and data and ensure that only authenticated and authorized users have access to the information stored in the FMS-NG system environment. Ex-Im Bank policy, including Rules of Behavior, ensures that users understand their responsibilities with respect to the information they are authorized to access. The access control system authenticates users and authorizes specific actions and cases/transactions requested by system users based on explicitly defined responsibilities. Roles are linked to the specific actions required to perform each user's official business function. The FMS-NG system application does not permit direct browsing or data mining of the internal data. All data access takes place via the user interface with all the applicable user access controls and access logging imposed by the application.

Direct access to the FMS-NG system Oracle database, bypassing the FMS-NG user front end, is prohibited to all FMS-NG business users. Only a small number of explicitly authorized Oracle Database Administrators (DBAs) have access to these databases outside of the application front end. Oracle DBAs hold a professional trust position and have undergone a NACI before being assigned to support the FMS-NG system. DBA actions are logged for later review as needed.

In addition to the access controls and policy protections, the FMS-NG system identifies error events, generates alerts and system logs, retrievable by the Bank's IT staff (including IT Security), that allow to determine whether unauthorized actions are being attempted and by whom. System policies are in place to investigate unauthorized activities on the system. These conditions of use are established for all authorized users at the time of user account creation and remain in force as long as the account is active.

As stated in response to (3), the entire Bank's staff (employees and contractors) must complete a background check - National Agency Check with Inquires (NACI) as a condition of employment at the Bank. Each employee completes mandatory annual training in IT security awareness and government employee ethics, which includes training in handling of PII data. Senior employees are required to submit an annual financial disclosure form. All contractors are annually required to complete the Bank's IT security awareness and to sign a Non-Disclosure Agreement (NDA). As such, the Bank's staff is considered to be "trusted insiders," knowledgeable about the Bank's policies and procedures, with an understanding that authorized access to the Bank's IT systems cannot be used for unauthorized purposes.

5. Does the program or application collect or store information related to a customer or employee where data is retrieved by name, unique number, symbol, or other identifier assigned to the customer or employee?
Yes. Customer, employee, and banking information is stored in FMS-NG and can be retrieved by name, unique number, symbol, or other identifier assigned to the Ex-Im's business partner (including individual sole proprietors) or employee. OCFO staff (e.g., Cash Control) have access to employee and business entity financial identifier information (ABA Routing Number, Account Number, and SSN or EIN) that is contained in FMS-NG.

a. Do other systems share data or have access to data in this system? If yes, explain.
Yes. The Department of Treasury Electronic Funds Transfer (EFT) payment Secure Payment System (SPS) directly receives information from FMS-NG as required to process and execute a payment to the Bank's employee, customer, or business partner.

b. Who will be responsible for protecting the privacy rights of the external users (customers) affected by the system?

FMS-NG system users and administrators are responsible for enforcing FMS-NG security and the appropriate use of the PII data. The Senior Agency Official for privacy will identify the individual responsible for protecting the privacy rights of external users/customers.

6. Who else will have access to the data?

*a. Will **other agencies share data or have access to data in this system** (International, Federal, State, Local, Other)?*

Yes. Two U.S. Department of Treasury systems indirectly have access to FMS-NG data. In both cases the summary data provided to these systems contains no PII:

1) Foreign Credit Reporting System (FCRS) on a quarterly basis; and
2) Electronic Certification System (ECS).

Summaries of data are extracted from this FMS-NG and shared for search and display on the Federal Funding Accountability and Transparency Act (FFATA) web portal (https://www.fsrs.gov/) in compliance with the FFATA http://www.whitehouse.gov/sites/default/files/omb/open/Executive_Compensation_Reporting_08272010.pdf). The extracted summary data does not contain PII.

From time to time, the Bank will also summarize data from this system in such documents as the Bank's annual report and periodic reports to Congress and the OMB. Any data included in the preparation of FFATA data extracts and other reports do not contain PII.

Information stored on the FMS-NG system and/or submitted by the Bank's customers is treated as business confidential information. Once an offer of a Bank product has been accepted by a Business, the information retains its business confidential status; however, the information may be disclosed in response to Freedom of Information Act (FOIA) requests, or be disclosed through other federally sanctioned process, as required by law. Such requests are handled by the Bank on a case-by-case basis. The affected businesses or individuals will have advanced notification of the information requests affecting them and will have an opportunity to specify which information is considered proprietary. Ex-Im Bank reserves the right to make a final determination to release information that is responsive to a FOIA request.

b. How will the data be used by the agency?

FMS-NG data will be used by Treasury for payment processing and legally required Federal Reporting. FMS-NG tracks credits fromobligation through maturity and termination. The FMS-NG system processes loans, guarantees, and insurance policies from obligation through final disbursement/payment, write-off, or Claim/Rescheduled Debt Servicing System application creation. It includes Ex-Im Bank's cash control system and standard general ledger. As described above, the data contained in this application may be extracted and summarized in statistical and textual summaries and reports that do not identify the individuals or the Company's business confidential information. Additionally, summarized extracts of the data will be shared for search and display on the FFATA web portal, at which point the summary data will not contain any PII.

C. 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, all of the data obtained for the processing of loans, guarantees, and insurance policies from obligation through final disbursement/payment and for providing complete loan and guarantee servicing over the entire life of credit, is both relevant and necessary to serve the Bank's customers. In order to minimize the public burden as well as the unnecessary collection and

retention of PII data, all FMS-NG system applications are designed to request and record only the relevant information for the conduct of Ex-Im Bank's business.

2. What personal information and/or personally identifiable information does the system contain?
The FMS-NG contains individual's personal information as listed in Table 1, Enumeration of PII Data Collected.

Personal information may be stored in the FMS-NG application for employees of the Bank, private individuals, and business entities functioning as sole proprietorships. The sole proprietors, acting in their capacity as corporate officials, may supply personal information including name, address, phone and fax numbers for their personal residence as well as individual Social Security Number (SSN) in place of an Employer Identification Number (EIN). Some sole proprietorship holders may also provide the ACH banking information for their personal Bank account instead of a corporate banking account. The Bank generally has no way of knowing that a sole proprietor is supplying personal contact information, in lieu of corporate contact information.

The application is used for reimbursements of Bank employees for travel and other direct costs that are incurred as a routine function of the Bank's business. In these cases, the application has the capability to store the employee SSN in the Tax ID field. For purposes of the reimbursement of an individual for pre-authorized expenses, only the banking information and NOT the SSN is retained in FMS-NG.

a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
No

b. Will the new data be placed in the individual's record (exporter or lender)?
Not applicable

c. Can the system make determinations about exporters or lenders that would not be possible without the new data?
Not applicable

d. How will the new data be verified for relevance and accuracy?
Not applicable

3. What controls are in place to protect information during consolidation?
Not applicable

b. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
Not applicable

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

Not applicable

4. How will the data be retrieved? Can data be retrieved by personal identifier? If yes, explain.

Primary access to the FMS-NG data will be via the FMS-NG forms and reports. FMS-NG users that have been granted access can retrieve data by personal identifiers (e.g. Customer's EIN and bank account number).

5. What are the potential effects on the due process rights of exporters and lenders of:

a. *consolidation and linkage of files and systems;*
No adverse impacts have been identified

b. derivation of data; accelerated information processing and decision making;
No adverse impacts have been identified

c. Use of new technologies.
No adverse impacts have been identified

D. Maintenance of Administrative Controls

1. *Does the system ensure equitable treatment of individuals or groups of people?*
   a. Explain how the system and its use will ensure equitable treatment of external users (customers).
   The application is neutral with respect to the equitable treatment of Ex-Im's business partners. The business entities (which may be individual sole proprietors) submit invoices to the Bank for payment for services rendered and products delivered. The application records the financial transactions that are associated with these payments. The application is designed with internal controls to facilitate the auditing of financial transactions processed by the application. The auditing capabilities allow the review of the Bank's FMS-NG use in order to assure equal opportunity for all Ex-Im customers.

   b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
   FMS-NG will be operated from a single site.

   c. *Explain any possibility of disparate treatment of individuals or groups*.
   No possibility of disparate treatment of individuals or groups attributable to the use of FMS-NG is known.

2. *What are the procedures for archiving and retaining information in the system?*
   a. What are the retention periods of data in this system?
   FMS-NG data is considered temporary Federal Record with the retention period subject to the applicable Record Schedules.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

FMS-NG is designed to mark the records inactive when no longer required for Bank business, whereupon these records become subject to the retention period as defined by the applicable Records Schedule. Records that are at the end of the specified legal retention period will be deleted by following the procedures documented in Oracle Financials Application Guides, based on the built-in criteria categories:

- Invoice Purge Criteria
- Payment Purge Criteria
- Supplier Purge Criteria
- Requisition Purge Criteria
- Purchase Order Purge Criteria
- Supplier Schedules Purge Criteria
- CUM Period Purge Criteria

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

FMS-NG will be the Banks financial system of record. The "feeder" applications (i.e., Comprizon, APS, EOL and MDM) are used to create, update, and maintain corporate information involving the customers/exporters and service or goods providers with an ongoing business relationship to the Bank. This data is updated in these applications at various times (e.g., policy renewal or as a result of a D&B match). Each business entity attests to the currency, completeness, and accuracy of the data.

The access control measures and backup systems designed into the FMS-NG system environment ensures that the data remains accurate, relevant, timely, and complete. Any changes to the data recorded in the applications are recorded in event logs so that the user ID of the account that changed the data can be known.

3. Does the system use new technology and what are the impacts of this technology on privacy?

c. Is the system using technologies in ways that the EX-IM BANK has not previously employed (e.g. Caller-ID)?

No. FMS-NG is a COTS application that will be hosted by Oracle Managed Cloud Services (MCS) and is FedRAMP certified. Access to the application is via a web browser. Web application security has therefore been an important security control in preventing unauthorized access to or misuse of information stored in the system.

d. How does the use of this technology affect external user (customer) privacy?

There are no discernible impacts on user (customer) privacy.

4. Does the system provide the capability to track and monitor individuals or groups?

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

No

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No

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

Only authorized users have active accounts that permit them to authenticate for access to the FMS-NG system. All user access and activity is logged and tracked by the system. Authorization to perform transactions on the FMS-NG system applications is governed by a role-based security model in which the FMS-NG system access controls restricts authorized users to only those types of transactions which are assigned to the business unit of which they are a part.

The Bank's staff (employees and contractors) is hired having successfully completed a background check and national agency check. Each employee completes mandatory annual training in IT security awareness and government employee ethics. Senior employees are required to submit an annual financial disclosure form. All contractors are annually required to complete the Bank's IT security awareness training and to sign a Non-Disclosure Agreement (NDA). Therefore, the Bank's staff is considered to be "trusted insiders," knowledgeable in the Bank's policies and procedures, and understand that authorized access to the Bank's IT systems cannot be used for unauthorized purposes.

5. How will the information in the system be secured?

a. What are the security controls (administrative, technical, and operational) controls designed to secure the system?

- The PII information in FMS-NG will be stored encrypted in place.
- Https protocol is employed in accessing FMS-NG.
- Oracle E-Business Suite implements built-in security components - *authentication, authorization* and an *audit trail*.
    - Authentication validates the user's identity, authorization controls the user's access based on responsibilities assigned, and the audit trail keeps track of the user's transactions to ensure that the user's privileges are not being misused.
    - Authorization - Oracle Application Object Library Security - consists of two main components – Function Security and Data Security. Function Security restricts user access to individual menus of functions, such as forms, HTML pages, or widgets within an application. Data Security restricts the access to the individual data that is shown once a user has selected a menu or menu option.
    - User and Data Auditing – auditing of users and changes they make to application data.

b. Is the system designated a 'system of records' under the Privacy Act, 5 U.S.C. 552a.

Yes.