Privacy Impact Assessment for FPPS

A. Introduction

The Export-Import Bank of the United States (EXIM Bank) is migrating its personnel and payroll administration to the Department of Interior's (DOI) Federal Personnel and Payroll Systems (FPPS) and Time and Attendance system known as Quicktime. This will enhance EXIM Bank's ability to better provide payroll and time and attendance services for its employees in a more efficient manner. EXIM Bank will rescind current personnel and payroll Systems of Records Notices (SORN) as they cease being operational after the migration is completed.

B. Data in the System

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

The FPPS is an online personnel and payroll system providing support to Federal agency customers and managed by the DOI's Interior Business Center (IBC). FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. FPPS allows for immediate updates and edits of personnel and payroll data. FPPS also handles regulatory requirements such as specialized pay, garnishments, and special appointment programs. FPPS also operates in batch mode for performing close of business, payroll calculation, and other processes. FPPS customers can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. FPPS is a major application that consists of several minor applications to include time and attendance applications, a system for creating retirement cards and updating retirement records, a system for converting client data for integration into FPPS, and a data warehouse that provides reporting functions for human resources departments.

Bi-weekly payroll information is migrated from FPPS to EXIM Bank's FMS-NG for entry into the EXIM Bank general ledger. No PII is migrated as part of this process.

Additional applications hosted on the FPPS system and covered under this privacy impact assessment are as follows:

- QuickTime. Online web-based time and attendance application that can be customized by EXIM Bank for requested functionality and to comply with agency policy. QuickTime provides ability to input, validate, and certify time and attendance data for transmission to FPPS. PII includes Social Security number (SSN), name, and user ID on Federal employees.
- Datamart. Online web-based reporting environment that can be used by EXIM Bank. Datamart provides the user the ability to query, analyze, chart and report data on Federal employees, retirees, volunteers, casual and emergency workers. PII includes SSN, name, Employee Common Identifier (ECI), home address, phone numbers, emergency contact information, medical and family leave, education, ethnicity and race, disability code, marital status, age, user IDs, involuntary debt (e.g. garnishments, child support), court orders, back pay, and individual bank routing numbers and account numbers.

The FPPS system data contains Personally Identifiable Information (PII) on EXIM employees.

The identifying data for individuals, such as their name and residential address information, may be linked in the FPPS system to:

- The individual's Social Security Number (SSN),
- The individual's banking information, or
- Both the SSN and the banking information.

Below are the PII Data Elements housed in FPPS.

Name, Citizenship, Gender, Birth Date, Group Affiliation, Marital Status, Other Names Used, Truncated SSN, Legal Status, Place of Birth, Security Clearance, Spouse Information, Financial Information, Medical Information Disability Information, Education Information, Emergency Contact, Race/Ethnicity, Social Security Number (SSN), Personal Cell Telephone Number, Personal Email Address, Home Telephone Number, Employment Information, Military Status/Service Mailing/Home Address. Taxpayer Identification Number; Bank Account Information such as Routing and Account Numbers; Beneficiary Information; Savings Bond Co-Owner Name(S) and Information; Family Member and Dependents Information; Professional Licensing and Credentials; Family Relationships; Age; Involuntary Debt (Garnishments or Child Support Payments); Court Order Information; Back Pay Information; User ID; Time and Attendance Data; Leave Time Information; Employee Common Identifier (ECI); Volunteer Emergency Contact Information; Person Number which is a unique number that identifies a person within FPPS; Person Number-Emergency which is a unique number identifying an individual within FPPS for a Leave Share Occurrence; and Person Number-Volunteer which is a unique number identifying an individual within the FPPS Volunteer Database.

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

Sources of information are generated by individual employees, employee resources and online database systems such as USA Staffing. Information 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 PL/SQL procedural upload to the FPPS database.

FPPS has interconnections with other Federal agencies; private organizations; Federal agency customers; state, city and county governments; and IBC internal systems. FPPS client agencies can use a web-enabled interface, WebFPPS, to access FPPS through a web browser to perform personnel and payroll tasks. The FPPS functionality of certain applications are only accessible via the IBC or EXIM intranets, and interconnections with the FPPS are outlined in Interconnection Security Agreements and/or Memorandums of Understanding. Authorized users (supervisors, HR specialists, security, and facilities) can track vacancies and view the entry on duty date and location for new hires through real time interfaces with FPPS and other automated staffing systems such asMonster's Enterprise Hiring Management and OPM's USA Staffing.

3. What is PII used for?

PII collected and maintained in FPPS is used to support full suite HR and payroll functions for EXIM Bank. FPPS also processes PII to manage regulatory requirements such as specialized

pay, garnishments and special appointment programs. PII is used for fiscal operations for payroll, time and attendance, leave, insurance, tax, retirement, debt, budget, and cost accounting programs; to prepare related reports to other Federal agencies including Department of the Treasury and the Office of Personnel Management; for reporting purposes to management and for human capital management.

B. Access to the Data

1. With whom will the PII be shared?

Data will be accessed by officials and employees of EXIM Bank in the performance of their official duties, including, but not limited to, employees of the Division of Human Capital, Office of General Counsel, Office of the Chief Financial Officer and the Office of Inspector General. EXIM Bank employees will have access to their own data. EXIM Bank is sharing this data with IBC as the service provider for FPPS. Additionally, FPPS data is shared and reported to other Federal agencies, including the Department of the Treasury and the Office of Personnel Management, as required for human resources, payroll, and tax purposes. FPPS data may be shared with the Department of Justice in the event information is required for litigation or law enforcement purposes and to any administrative State or Federal court in a relevant litigation matter (subject to appropriate process). FPPS data may be shared with other Federal agencies pursuant to applicable law. FPPS data will be shared with National Archives and Records Administration for record management inspections in its role as Archivist; FPPS data will be shared in the event of data breach and for mitigation response.

Disclosure may be made to a Congressional Office from the record of an individual in response to an inquiry from the Congressional Office made at the request of that individual.

FPPS data is not used in any matching programs.

Disclosure to consumer reporting agencies:

Disclosures pursuant to 5 U.S.C. 552a(b)(12). Disclosures may be made from this system to "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

2. Describe the contractor/third party and how the data will be used.

N/A

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

Yes, Federal employees have the option of not providing information on forms required during the application and onboarding process. These official forms contain Privacy Act Statements notifying individuals of the authority, purpose and uses of the information. Employees are required by law to provide certain types of information, such as name and SSN as a part of the employment process. This information is required by applicable Federal statutes, including tax and employment eligibility regulations, and are necessary data elements in FPPS.

Federal employment forms collect the following information that is required from an individual to be considered for Federal employment; however, declining to provide this information may affect the employment eligibility and selection of the individual:

- OF-306 - Declaration for Federal Employment. Some of the required fields include full name, SSN, date of birth (DOB), place of birth, felonies, military convictions, delinquent on federal debts.
- I-9 - Employment Eligibility Verification. Some of the required fields include full name, address, DOB, SSN, Citizenship, proof of identity (driver's license, U.S. passport, SSN card, etc.).
- Fair Credit Reporting Release - This document requires the applicant's signature in order for Personnel Security Services to obtain information for their background investigation to determine fitness for employment, security access, etc.

Below are forms that are requested but not required, and will not affect the employment eligibility and selection of the applicant:

1. SF-181, Ethnicity and Race Identification
2. SF-256, Self-Identification of Disability

4. What information is provided to an individual when asked to provide PII data?

Privacy Act Statements are provided when information is collected directly from individuals for entry into FPPS. For example, information is collected through forms that contain Privacy Act Statements, such as I-9, Employment Eligibility Verification. I-9 contains the following Privacy Act Statement:

> Authorities: The authority to collecting this information is the Immigration Reform and Control Act of 1986, Public Law 99-063 (8 USC 1324a).
>
> Purpose: This information is collected by employers to comply with the requirements of the Immigration Reform and Control Act of 1986. This law requires that employers verify the identity and employment authorization of individuals they hire for employment to preclude the unlawful hiring, or recruiting or referring for a fee, of aliens who are not authorized to work in the United States.
>
> Disclosure: Submission of the information required in this form is voluntary. However, failure of the employer to ensure proper completion of this form for each employee may result in the imposition of civil or criminal penalties. In addition, employing individuals knowing that they are unauthorized to work in the United States may subject the employer to civil and/or criminal penalties.
>
> Routine Uses: This information will be used by employers as a record of their basis for determining eligibility of an employee to work in the United States. The employer will keep this form and make it available for inspection by authorized officials of the Department of Homeland Security, Department of Labor, and Office of Special Counsel for Immigration-Related Unfair Employment Practices.

Individuals are also provided notice on how their PII is managed during these personnel and payroll activities through the publication of this PIA, systems of records notices published in the Federal Register and published government-wide system notices, such as OPM/GOVT-1, General Personnel Records.

5. How will data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

FPPS authorized users, including EXIM authorized Human Capital personnel, may retrieve information on an individual using full name, SSN and Employee Common Identifier (ECI).

Certain personnel within EXIM Bank and IBC, involved in operations and maintenance of FPPS payroll operations, can retrieve information on an individual using:

- ECI- unique number identifying employees across Federal automated systems
- SSN and full name
- Person Number - unique number which identifies a person within FPPS
- Person Number-Emergency - unique number identifying an individual within FPPS for a leave share occurrence
- Person Number-Volunteer - unique number identifying an individual within the FPPS volunteer database
- Taxpayer Identification Number (TIN) - unique number identifying the Trustee for the Estate of a deceased employee

6. What type of reports will be produced on individuals?

Reports can be produced on an individual containing many of the data elements in FPPS. FPPS also routinely generates a variety of reports related to employment that are required by law, such as Internal Revenue Service (IRS) forms (1099- MISC and W-2); reports of withholdings and contributions for benefits and union dues; and reports on individuals who are delinquent on child-support payments. Access to the reports is limited to employees who process or file the reports and individuals who are granted access on a need-to-know basis. Copies of the reports may also be provided to government entities as required by law, such as tax forms to the IRS.

Information about individuals whose data is in FPPS cannot be retrieved without knowing specific information about the employee. For example, information about a trustee, family member, savings bond co-owner, or beneficiary cannot be retrieved without knowing certain information about the employee.

FPPS has a special reporting system which provides statistical summaries of the workforce showing breakdowns by relevant demographics and comparison between the representation in specific agency occupations in the civilian labor force.

FPPS provides various employee and position management information reports. These reports may also be generated from data fed to IBC's Data Warehouse "Datamart/OBIEE." Datamart/OBIEE maintains the data integrity of FPPS so users will only be able to access records within their range of authorization as defined in FPPS.

FPPS also provides a security report that lists termination or change transactions affecting system users.

C. Attributes of the Data

1. How will data collected from sources be verified for accuracy?

Some data that is collected from new employees, such as name and SSN, is verified for accuracy using the U.S. Customs and Immigration Services' E-Verify system or directly with the Social Security Administration. Other information, such as bank account information, is verified for accuracy by requesting copies of supplemental supporting documents directly from the individual, such as a voided check which validates the bank account routing and account numbers. In some cases, information such as home telephone numbers and emergency contact information is not verified for accuracy. It is the responsibility of the individual to provide the accurate information.

FPPS contains validity and relational edits designed to ensure the data entry technician inputs accurate information. The payroll data fields have the capability to ensure that the data entered is correct and cannot be altered such as validating employee SSN and state abbreviations; restricting the deletion of addresses; and requiring the use of numeric dates.

Without valid data elements, actions cannot be processed by FPPS. IBC's Payroll Operations Division (POD) requires authorized documentation from clients, or relies on regulatory requirements (i.e., tax law changes), before making adjustments to data in the system.

Where feasible, data entry modules in FPPS utilize a variety of data integrity validation controls to limit data entry errors, such as drop down menus, check boxes, text field size limitations, and predefined formats. A field may also use an edit mask to force entry of an SSN 999999999 as 999-99-9999 or the date 20000114 as 2000/01/14.

During Quicktime processing, time and attendance (T&A) data transfers into FPPS. The mainframe executes an Oracle SQL script to flag records that have been uploaded to FPPS to avoid duplication of data. After Quicktime bi-weekly processing is complete, a regularly scheduled job is run from Quicktime servers to generate the results of the bi-weekly mainframe run. All results including errors are included in this file. In addition, an output file is generated to capture any specific T&A errors. IBC will review the applicable T&A errors file and make necessary if corrective actions.

2. How will data be checked for completeness?

EXIM Bank can request FPPS to configure the system to make data fields mandatory or optional. If a data field is mandatory, data validation checks, such as a block on creating a new record, are employed to ensure that all mandatory data is entered. The user can bypass an optional field by pressing the 'Enter' key.

EXIM Bank will implement additional procedures to verify the accuracy and completeness of the information that is provided on behalf of their agency. In some cases, the information provided by individuals is not verified, and the individual providing the information is responsible for the accuracy of the information that is supplied.

In addition, IBC servicing personnel and EXIM managers and staff will perform various functions to check data for completeness, such as the following:

- Review and edit data to ensure that all required fields are populated, complete, and in conformance with Federal government personnel rules.
- Review records to validate the existence and completeness of time and attendance records for all active employees for the current pay period.
- Edit payroll transactions to ensure all required fields are populated and complete.
- Monitor time and attendance records to ensure these records have been received from the time and attendance modules.

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

Data in FPPS must be maintained in a current state in order to perform the system's human resources and payroll functions. EXIM Bank is responsible for keeping the data they provide up to date, including establishing procedures for updating data. The system also employs various data validation controls to ensure that data entered into the system is current. These data validation modules can notify Human Capital Division designated Data Custodians if certain data has been held in excess of a certain amount of time without an update.

The Employee Express interface with FPPS allows employees the opportunity to input data for many types of personal transactions which are loaded into FPPS on a regular basis. The effective date of the transaction initiated in Employee Express is based on the type of transaction, when it is initiated, and whether a transaction is starting or stopping an action. Therefore, if the transaction affects payroll, it may or may not be implemented for the pay period in which the transaction was entered based on the effective date.

FPPS runs a number of processes daily and other designated times (e.g., close of business, paid dailies, one-time adjustments, T&A gathers, pay calculate, etc.) to compile transactions and help to ensure all personnel and payroll data is current.

There are no documents that describe all FPPS edits and validations or interface file agreements, which help to ensure data is current. This information is contained in design documents, the online help system, and within the FPPS codes.

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

Records maintained in FPPS belonging to EXIM Bank are retained in accordance with the General Records Schedules (GRS) approved by the National Archives and Records Administration (NARA). Retention and disposition may vary based on the type of record and needs of the agency. FPPS data is covered under General Records Schedule 1 "Civilian Personnel Records" and Schedule 2, "Payrolling and Pay Administration Records". These schedules have various retention options for different types of data.

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

EXIM Bank maintains records as needed under NARA-approved records schedules for the retention of reports and data. While the IBC provides system administration and management support to agency clients, any records disposal is in accordance with customer agency approved data disposal procedures.

EXIM Bank is responsible for purging employee data according to the customer agency records schedule after an employee's access authority is terminated or the employee retires, changes jobs, or dies. The IBC may purge or delete any customer payroll or personnel records if it is a requirement of the customer agency and as agreed upon in the Inter-Agency Agreement with the IBC.

IBC records are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and DOI's 384 Departmental Manual 1.

6. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are risks to the privacy of individuals due to the volume of sensitive PII contained in the system. FPPS supports a full suite of human resources functions, including calculating payroll. The data in FPPS is necessary to perform those functions and to comply with related Federal laws and regulations. To prevent misuse, (e.g., unauthorized browsing) EXIM Bank signed a Service Level Agreement (SLA) with the IBC to clearly establish and document IBC and client security roles and responsibilities. Most of the employee data in FPPS is collected from individuals and entered into FPPS by an authorized Federal human resources professional with access to the system.

The FPPS system has undergone a formal Security Authorization and Accreditation and has been granted an authority to operate by DOI in accordance with FISMA and NIST standards. FPPS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

Data is maintained to support agency personnel and payroll operations in accordance with approved records retention schedules. The retention and procedures for disposition for FPPS data is covered under General Records Schedule 1 "Civilian Personnel Records" and Schedule 2, "Payroll and Pay Administration Records."

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The IBC follows the least privilege security principle, such that only the least amount of access

is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user.

EXIM Bank employees are required to complete annual security and privacy awareness training, and EXIM Bank personnel authorized to manage, use, or operate the system information are required to take additional role-based training developed and offered by IBC.

D. Maintenance, Administrative Controls and Risk

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

The FPPS data is both relevant and necessary. FPPS supports a full suite of human resources functions, including calculating payroll. The data in FPPS is necessary to perform those functions and to comply with related Federal laws and regulations.

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

The cumulative data figures described above will become part of each individual's record, and will be used for payroll and various types of reporting.

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

IBC has procedures in place to validate pay data calculations, make timely disbursements, and correct errors to ensure the employee receives an accurate paycheck. Various validation tools help identify processing discrepancies so that adjustments can be made as appropriate. Any necessary corrections to payroll are completed on a daily basis both prior to and after the payroll calculation process.

<u>Time and Attendance (T&A)</u>

EXIM Bank timekeepers and certifiers confirm accuracy of data before it is sent to IBC.

Once the T&A data has been loaded into FPPS, the IBC reviews the data to determine whether T&A records are missing. IBC notifies EXIM Bank of missing T&A records so that the client may send in the missing data prior to the bi-weekly calculation.

IBC analyzes and reviews any FPPS error messages that may be a result of input of inaccurate data. The edits invoked in FPPS on T&A data identify most T&A errors that would result in incorrect or incomplete pay. The IBC staff researches inaccuracies prior to processing payroll calculations and resolves errors where possible. IBC relies upon authorized input (i.e., signed timesheet) from EXIM Bank in order to resolve any problems with T&A. No correction or adjustment is made in payroll without an authorization, (either by law or regulation), or an authorized document provided by EXIM Bank. This authorization procedure applies to changes that are requested by an individual client employee as well as changes/procedures requested by EXIM Bank.

<u>Employee Express</u>

Employee Express is an online employee self-service program made available by the Office of Personnel Management that allows the individual to make certain changes to their payroll or personnel data. Occasionally, the interfacing transactions fail and do not update FPPS correctly. The IBC receives daily Employee Express interface error listings that are reviewed within the current pay period and the status of resolution is tracked during the bi-weekly review performed by the IBC supervisor and lead.

Payroll Calculate Processing

After the bi-weekly calculate, the IBC reviews FPPS reports daily to identify any incomplete or inaccurate payments that were made. Inaccurate payments may occur when T&A or other authorizing documentation was not received by IBC prior to processing payroll calculate. Based on the type of error, IBC will contact either the employee's timekeeper or Servicing Personnel Office (SPO) to start the process of correcting the employee's record. Depending on the type of corrective action processed the IBC Payroll Operations Branch (POB) can make a supplemental payment (paid daily) to the employee after the payroll calculating process has been completed for the current pay period. Before processing a paid daily, IBC requires an amended T&A or confirmation that the SPO has completed the corrective personnel action. IBC procedures require that authorizing documentation from the client support all corrections made in the system. Corrections and adjustments are reviewed by a supervisor, lead, or Payroll Program Technician. The following pay period, during the recompensation review process, IBC processes the corrected T&A or personnel action for payment while offsetting the paid daily payment. This completes the corrective cycle and ensures a correct pay record for the employee. Source documentation is maintained for each action taken by payroll. Most documentation is electronically imaged and maintained indefinitely in the POB Document Retrieval System.

The Certifying Officer (CO) uses the Threshold Exception listing to support the validity of the bi-weekly disbursements being scheduled for payment that exceed a predetermined dollar threshold. The CO may conduct research if the payment is not included on the Threshold Exception listing to determine whether it is a valid override of the threshold or may choose to suspend the payment, removing it from the disbursement schedule altogether to be further analyzed to determine if it is a valid payment. IBC logs and tracks work activities in FPPS to resolution.

Federal Employment and Income Taxes

FPPS provides a report to the IBC's Review and Analysis Branch (R&A) that summarizes all federal tax withholdings and contributions. Tax Accountants within R&A reconcile this report bi-weekly to the general ledger to ensure that all federal employment and income taxes are accounted for and will be paid correctly.

The taxes and earned income credit (EIC) payments are entered manually into the Electronic Federal Tax Payment System (EFTPS) once the bi-weekly payroll taxes are reconciled to the general ledger. The payment is authorized to be issued to the Internal Revenue Service (IRS) after all data is verified. The payment is issued by Treasury through EFTPS.

U.S. Treasury's (Treasury's) CA$H-LINK II system is used to confirm that the payments were issued. Once the payment has been confirmed in CA$H-LINK II, an entry will be made into the accounting system to record the payment.

4. Who will have access to data in the system or electronic collection?

EXIM Bank employees will have access to their own data. EXIM Bank Human Capital staff will have access to all data, as appropriate, in the FPPS. Access to the data in the system will be granted by FPPS system administrators, programmers, developers, analysts, database administrators, payroll operations staff, and others (who may be contractors) supporting the system and performing system maintenance and other related activities and may have access to the data in the system.

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

EXIM Bank has an appointed a Human Capital Data Custodian who is responsible for granting access to their agency's FPPS data. The Data Custodian appoints Security Points of Contact (SPOC), who can set and restrict data access privileges for system users. Access for Data Custodians and SPOCs is granted by the IBC through the Decentralized Security Administration Facility (DSAF) application. The DSAF controls access to the mainframe computer that hosts FPPS.

The following three forms that contain relevant guidance are used for delegating access and rights to Data Custodians and SPOCs:

- DEN-NBC-IT-01: Data Custodian Responsibility Statement
- DEN-NBC-IT-02: Data Custodian and SPOC Designation
- DEN-NBC-IT-03: SPOC Responsibility Statement and Rules of Behavior

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

Yes. IBC manages its systems, including contractors, independently of EXIM Bank and are subject to IBC's privacy requirements.

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

IBC strictly manages individual privacy compliance of its employees and contractors.

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

No

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

No.

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

N/A

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

FPPS monitors authorized users by maintaining an audit trail of activity. The audit trail includes the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls.

IBC fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any FPPS equipment. The use of DOI IT systems, including FPPS, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security (IBC-EXIM Bank).

12. ***How will the PII be secured?***

EXIM Bank controls are as follows: Physical Controls. Security Guards, Locked files, secured facility, identification badges, and locked offices.

IBC controls are as follows: Physical Controls. Security Guards, Locked files, secured facility, closed circuit television, cipher locks, identification badges, and locked offices.

Technical Controls: Password, firewall, encryption, User Id, Intrusion Detection System, Virtual Private Network (VPN), Public Key Infrastructure (PKI) Certificates, Personal Identity Verification (PIV) Card.

Administrative Controls: Periodic security audits, backups secured off-site, Rules of Behavior, role-based training, regular monitoring of users' security practices, methods to ensure only authorized personnel have access to PII, encryption of backups containing sensitive data, mandatory Security, Privacy and Records Management Training.

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

The IBC Office of Human Resources, Deputy Chief Financial Office Director serves as the FPPS Information System Owner and the official responsible for oversight and management of the FPPS security controls and the protection of customer agency information processed and stored by the FPPS system. The Information System Owner and the FPPS Privacy Act System Manager

are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in FPPS.

System users and administrators are responsible for protecting the privacy rights for the public and employee to protect and ensure the use of PII data. The EXIM Bank Senior Agency Official for Privacy (SAOP) is responsible for addressing privacy complaints and redress or amendment of records.

14. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The FPPS Information System Owner is responsible for oversight and management of the FPPS security and privacy controls, and for ensuring to the greatest possible extent that FPPS customer agency and agency data is properly managed and that all access to customer agency and agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to the customer agency and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures.

EXIM Bank Director, IT Security and System Assurance will report the potential loss, compromise, unauthorized access or disclosure of data resulting from EXIM Bank's activities or management of the data to the EXIM Bank's Senior Agency Official for Privacy, IBC and US – CERT promptly.

Authority

The Export-Import Bank is authorized to request this information pursuant to the following: Authority of the Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 et seq.); 5 U.S.C. 5101, et seq., 5501 et seq., 5525 et seq., and 6301 et seq.; 31 U.S.C. 3512; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers. 31 U.S.C. 3512 et seq.; and 5 C.F.R. Part 293.