PRIVACY IMPACT ASSESSMENT

INTRODUCTION

The objective of the Privacy Impact Analysis (PIA) is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing or processing sensitive, personal data that may be considered private. Upon completion of the questionnaire and acquisition of signatures, please return to DIT Information Security Staff located in Virginia Square, Room Number A7032.

Agency: Federal Deposit Insurance Corporation (FDIC)

System Name: FDIC/NFC Payroll/Personnel FOCUS Download Processing

System Acronym: PAYPERS

System Owner/Division or Office: Division of Information Technology (DIT)

A. Information and Privacy

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

C. System Description

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

PAYPERS is a Payroll Personnel computer application that contains FDIC payroll related data. This data is transmitted from the National Finance center (NFC) to the FDIC on a weekly basis. PAYPERS data is stored in files on the FDIC mainframe, and is available for retrieval by other FDIC applications. PAYPERS reports are also produced and distributed to about 25 FDIC personnel.

D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

   Full Name, Social Security Number, Date of Birth, and Address are contained in PAYPERS.

2. Can individuals "opt-out" by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

   ☐ Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

   ☒ No Explain: NFC is the system-of-record from which the PAYPERS system imports data. As a secondary system, individuals cannot "opt-out" from providing SSN, full name, date of birth, and addresses. Additionally, the purpose of PAYPERS is to allow other authorized FDIC systems access to imported NFC data. PAYPERS itself, however, does not use NFC data, PII or otherwise. Accordingly, the use of the PAYPERS-imported, NFC data would be addressed by the NFC PIA.

3. What are the sources of the information in the system? How are they derived? Explain.

   The source of this data is the National Finance Center (NFC). This data is derived from FDIC payroll information that NFC has processed.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

   The National Finance Center (NFC) provides this data to the FDIC. The purpose for providing this data is primarily to reconcile payroll-related NFC and FDIC data. In addition, PAYPERS data is used in the following ways:

- **Personnel Data (D0PPAY, D0PPAY7):** This data is downloaded every Monday and Wednesday in two separate files. From this data, biweekly datasets are created as requested by the New Financial Environment (NFE), Budget, Equal Employment Opportunity (EEO), DOF, and DIT.
- **Current Pay Status (CURPAY):** This data is downloaded every Monday and Wednesday.
- **Organizational Structure Code Table (ORGTABLE):** This table is downloaded every Monday and Wednesday.
- **PMSO data (D0PMSO2, D0PMSO):** This data is downloaded every Monday and Wednesday from NFC's Position Management System (PMSO).
- **NFE Financial Data (DWNNFE2):** This data is downloaded on the second Monday of each pay period. This data is combined with the personnel data to create a flat file that is used in the Travel system and NFE by DOF.
- **FAST personnel data (FASTOASI):** The data was originally downloaded to the FAST application which was retired in 2002. The download is run on the second Monday of each pay period and is now used to update the (Overarching Automated System) OASIS for DRR.
- **MRNO data (D0MRNO):** The master record data from the PMSO file id downloaded every Monday and Wednesday.
- **Thrift Savings data (THRIFT):** This data is downloaded on the second Monday of each pay period.
- **Flexfund data (FLEXTA):** This data is downloaded on the second Monday of each pay period.
- **Taxable fringe benefit data (LI415):** This data is downloaded on the second Monday of each pay period.
- **COMP Leave Balances (DWN497):** This data is downloaded on the second Monday of each pay period and combined with the personnel data to create a file for DOF.
- **LWOP data (TALOOP2):** This data is downloaded on the second Monday of each pay period to create a report on the FDIC's mainframe.
- **FDIC Staffing/Distribution reports (GROUPTST):** This report is submitted on the second Monday of each pay period on the NFC's mainframe to create multiple reports for DOF-Budget.
- **Flexfund Plan report (IPFFUN3A):** This report is downloaded on the second Monday of each pay period to create the report in an ASCII format.

- **Sick Leave report (GROUPSCK):** This report is not downloaded but submitted on the second Monday of each pay period on the NFC's mainframe to create a report for the Health Unit.
- **T&A Leave Balances & Time-Off Awards (TOA) data**: The leave balances from the prior pay period processing cycle are downloaded from NFC and loaded into Corporate Database BASE 051.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

   None

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

   None

E. Access to Data:

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

   FDIC employees who have been granted access to PAYPERS data. This includes users, managers, and system administrators. Contractors and developers only have access to sanitized PAYPERS data in the FDIC development environment. (i.e. PAYPERS data cleaned up to have only test SSNs and Names)

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

   Access to the data is determined by the data owner DIT. Yes, Criteria, procedures, controls, and responsibilities regarding access are documented by DIT.

   Yes, the DIT manager must approve access to PAYPERS.

   The process begins with filling out an Access Authorization Security Application (AASA) request for PAYPERS.

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

   Access will be restricted to specific files requested through AASA.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

   The FDIC requires annual security training of all employees and contractor staff. In addition, secure passwords, time-out screen locking, and shredding of sensitive documents are tools that FDIC utilizes to further ensure sensitive data is properly protected.

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

   Yes, other FDIC applications require access to this data. See section D.4. above for detailed explanation of purposes and needs for PAYPERS access.

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

   The FDIC DIT security group has established common security rules and guidelines for protecting the public, as well as, FDIC employees. In addition annual privacy training is mandated.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

   NFC uses this data to produce payroll for the FDIC. Both NFC and FDIC have established the criteria for what data can be shared through a Memorandum of Understanding (MOU) agreement. Non-disclosure agreements are in place. The need to share PAYPERS data is so NFC and FDIC can reconcile FDIC payroll-related data. (Refer to D.4. above for specifics.)

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

   The DIT Chief Privacy Officer, DIT Security Manager, DIT Project Manager, and the DIT Program Manager will hold primary responsibility for assuring proper use of this sensitive PAYPERS data. Yes, these individuals are fully accountable. In addition, ultimately, all FDIC employees and contractor staff that are granted access through AASA are also responsible and accountable to uphold the FDIC's highest standards regarding sensitive data.

9. Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the corporation be affected?

   FDIC has given the highest priority to protecting our sensitive data, since serious harm could result if PAYPERS data became compromised.

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

    The contractor staff will have responsibility for the design and maintenance of PAYPERS. Yes, contractor confidentiality agreements and non-disclosure agreements are in place.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

    Yes, the FDIC data owner DIT has been contacted regarding PAYPERS. DIT has verified that NFC is the only agency currently having access to PAYPERS data.

F. Accuracy, Timeliness, and Reliability

1. How is the data collected from sources other than FDIC records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for making this determination? Explain.

   PAYPERS data is collected from the NFC weekly data feed is verified by FDIC personnel. FDIC uses Secure DCONNECT software to ensure safe, reliable and secure transmission from NFC to the FDIC.

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

   PAYPERS data is checked for completeness by Secure DCONNECT software generating an e-mail when the transmission from NFC to FDIC is successful. In addition, FDIC personnel perform checks of payroll-related FDIC data to ensure accuracy. Technology plus experienced FDIC employees are important sources for ensuring the completeness and accuracy of PAYPERS data.

G. 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? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

   Yes. Yes. Yes, all PAYPERS documentation can be found in the FDIC Star Team Repository.

2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

   No. Steps taken included checking with DIT and verifying no new data is planned for PAYPERS at this time.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

   No, since no new data is planned for PAYPERS at this time.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

   No consolidation of PAYPERS data is planned at this time. No.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

   Retrieval of PAYPERS data is done manually through looking at PAYPERS reports or files. No on-line retrieval is possible at this time in PAYPERS. However, other FDIC applications load PAYPERS data and allow retrieval by a personal identifier. (e.g. SSN). See section D.4. above for more information.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

   A variety of payroll-related reports are produced weekly for PAYPERS. These reports are used by DOF, DIT, and DRR to reconcile NFC and FDIC payroll-related data. See section D.4. above for the specific use of these PAYPERS reports. Only approved personnel in DOF, DIT, and DRR will have access to these PAYPERS reports. These reports are distributed weekly through the FDIC internal mail, and monthly through encrypted e-mail to the DIT Help Desk and Field Office Representatives mailboxes.

H. 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? Will the same controls be used? Explain.

   The PAYPERS system only operates at one site. N/A

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

   The FDIC has a Records Retention Schedule of 10 years for PAYPERS data. Retention periods were determined based upon the NARA retention period guidelines. DIT management has set these guidelines for retention periods of PAYPERS data.

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

   FDIC has established common procedures for the disposition of data at the end of the retention period. PAYPERS reports will be maintained for a period of 10 years. The PAYPERS reports are shredded when they are no longer needed. The DIT Security Group has established these procedures.

4. Is the system using technologies in ways that the Corporation has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

   Yes, Smart Card technology has been implemented to protect FDIC PAYPERS sensitive data.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

   The use of this technology ensures that the person logging has been issued smart card access. No, this technology will not introduce any new compromise, on the contrary, it will improve privacy protection.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

   Yes, monitoring of access to PAYPERS data on the FDIC mainframe is being performed daily through Access Control Facility (ACF2) logging. Data collected includes Logon ID of person accessing PAYPERS data, along with, functions performed and date and time of access.
   Yes, system administrators have monitoring turned on so they can review PAYPERS file access.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

   N/A

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

   Financial Information Management Records - #30-64-0012
   Unofficial Personnel System - #30-64-0015

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

   N/A

I. Business Processes and Technology

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

   Not at this time.

2. Does the completion of this PIA potentially result in technology changes?

   No.