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: **MyEnroll**

System Acronym: **MyEnroll**

System Owner/Division or Office: **Division of Administration (DOA)**

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.

MyEnroll.com (MyEnroll) is a proprietary external website operated by Benefit Allocation Systems (BAS), Inc. The website allows FDIC employees to self-enroll and update their elections associated with the following Federal and FDIC benefits:

- Federal Employees Health Benefits (FEHB) Program
- Federal Employees Dental and Vision Program
- FDIC Premium Conversion Plan
- FDIC Choice, which includes the following FDIC-provided benefits:
  - FDIC Dental Insurance
  - FDIC Vision Insurance
  - FDIC Life Insurance
  - FDIC Long-Term Disability Insurance
  - FDIC Health Care and Dependent Care Flexible Spending Accounts (FSAs)

As a third party benefits administrator, BAS aids the FDIC in implementing and administering services related to the FDIC Choice flexible cafeteria benefits program, including claims processing for FDIC Health Care and Dependent Care Flexible Spending Accounts. BAS also supports the administration of Corporate University's Professional Learning Accounts, as well as a number of other benefit-related activities servicing FDIC retirees, which include:

a) billing and accounts receivable activities related to the FDIC Dental Insurance for Retirees (covering retirees and surviving dependents); and
b) support for FDIC's semi-annual reimbursement of a percentage of health premiums paid by certain retirees that accepted buyouts in years 1994 through 1996.

Additionally, the data maintained by MyEnroll is used to provide ongoing customer services, including a Benefits Hotline Call Center, communications functions, and various premium billing/collection activities associated with the administration of FDIC's benefits program.

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.

   MyEnroll contains information about FDIC employees that are eligible to participate in the FDIC's Benefits program DOA manually extracts employee information from the Corporate Human Information Resources System (CHRIS HR) and transmits the data securely via Secured File Transfer Protocol (SFTP) to BAS, daily, seven days a week, where it is imported into a BAS-maintained database. The following personal information is extracted from CHRIS HR and imported into the MyEnroll database: employee name, social security number, employee id, home address, birth date, compensation rate, job title, retirement plan, and retirement date. FDIC employees are also required to enter personal information about their dependents that participate in the FDIC Benefits program, including the dependent's name, SSN, Date of Birth, home address, and telephone number.

   In addition to the data obtained from CHRIS HR, MyEnroll contains information entered by FDIC employees via the MyEnroll website related to their benefit selections.

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
   ☒ No Explain:
   The personal information (as identified in D.1. above) for all eligible FDIC employees, is electronically transmitted from FDIC to BAS, whether or not the employees participate in the FDIC Benefits Program.

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

   Employee information (see the response to D.1 above) is extracted from the CHRIS HR system and electronically transmitted to BAS, where it is imported into the MyEnroll database. Additionally, employee benefit selections are manually entered into MyEnroll directly by FDIC employees via the MyEnroll website, as is personal information about the dependents of FDIC employees that participate in the FDIC Benefits program.

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.

Not applicable. No Federal agencies are providing data for use in the system.

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.

Not applicable. No state or local agencies are providing data for use in the system.

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.

Not applicable. No third party sources are providing data for use in the system.

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, retirees, and surviving dependents have access to MyEnroll. They require this access in order to verify their personal information, make updates to their benefits selections, and to make updates to information contained within MyEnroll about their covered dependents.

FDIC Human Resource Specialists within the Division of Administration (DOA) have administrative control over the system.

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 MyEnroll website is available to all FDIC employees who are eligible to participate in FDIC's Benefits program. FDIC employees can only access their own personal information, and their dependent information, and are able to update only their own benefit selections. They do not have access to information pertaining to any other FDIC employees maintained within MyEnroll.

The FDIC Human Resource Specialists within the Division of Administration (DOA) have administrative control over the system.

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

   FDIC employees' access is limited to their own personal information and their dependent's personal information, as well as their own benefits selections.

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.

   An FDIC employee's access is limited to their own personal information, information relating to their covered dependents, and any associated benefits selections. FDIC employees are not given access to browse information maintained for other individuals within MyEnroll.

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.

   As noted in Section D.1 of this PIA, MyEnroll obtains employee data from CHRIS HR, daily, seven days a week. This information is necessary for verification of eligibility and to process within NFC the Benefits selections made by FDIC employees. No other systems provide data to MyEnroll.

   BAS manually sends enrollment data to the insurance carriers via secure file transmission methods to process employees' benefits selections: To FDIC's dental and long term disability insurers, the files are sent via PGP encryption using the MetLife Web service. To FDIC's vision insurance carrier, VSP, BAS sends the files via PGP encryption using the VSP web service.

   MyEnroll exports data daily, five times per week, except federal holidays, to the National Finance Center (NFC), so that the employee benefits selections can be processed in FDIC's payroll. BAS transmits the enrollment election data manually in accordance with NFC's secure file encryption process, via VPN secure remote.

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.

   BAS will have overall responsibility for protecting the privacy rights of individuals whose information is contained in MyEnroll. In addition, those FDIC users having administrative control over the system are responsible for protecting the data to which that access provides. All FDIC employees are required to complete FDIC's Information Security Awareness training and Privacy Act Orientation training on an annual basis, which includes information relating to protecting the privacy rights of individuals.

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 receives data from MyEnroll in order to process the benefits selections of FDIC employees. An Interagency Service Agreement (ISA) is established between NFC and FDIC.

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 System Owner and Information Security Manager collectively hold primary responsibility for assuring proper use of data in the system. In addition, all FDIC employees and contractor staff who have access to the system are responsible and accountable for upholding the FDIC's standards regarding protection of personal and 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?

   The magnitude of harm to the Corporation would be low and the reputation of the Corporation would not be affected significantly if privacy related data is disclosed.

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 design and maintenance of the MyEnroll website and database are handled by BAS. BAS operates its website and database for many US government agencies. A Contract is in place with BAS that includes privacy, security and confidentiality requirements.

    Contractor involvement is not required to assist FDIC DOA staff in manually extracting the information from CHRIS and sending it to BAS.

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.

    Not applicable. MYENROLL does not share data with other agencies.

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 this making this determination? Explain.

   Not applicable. No data is collected from sources other than 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.

As noted in Section D of this PIA, some of the MYENROLL data is received from CHRIS. FDIC employees add to this data by making their benefits enrollment selections on the MyEnroll website, or by adding, updating, or deleting information on their dependents that may be participating in the FDIC Benefits Program. If an employee finds that his own data in MyEnroll is incorrect, he is instructed to contact the FDIC Human Resources Branch. Human Resources verifies the necessary data corrections are made into CHRIS; MyEnroll receives the corrected data daily from the CHRIS data file upload. The following technical controls within MyEnroll also ensure the accuracy of the data:

- Validation during data entry and processing
- Data validation occurring before data is committed into MyEnroll
- Using required fields to prevent critical data from being omitted.

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, the use of the data is both relevant and necessary to the purpose for which the system was designed. The data provided to MyEnroll by the FDIC is needed to ensure that eligible FDIC employees can make their benefits choices and their choices can be processed by NFC.

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.

   Not applicable. The system will not derive PII from any new data previously non-inclusive.

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

   Not applicable. The system cannot make privacy determinations about employees that would not be possible without new data.

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.

   Not applicable. Data is not being consolidated.

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.

   An FDIC employee can only retrieve his own enrollment data.

   Data Files to Insurance Carriers: Data is retrieved via MyEnroll's unique employee identifier. Social security number is provided in the data file because it is the unique identifier between MyEnroll and the insurance carriers system.

   NFC Files: Data is retrieved via MyEnroll's unique identifier. Social security number is provided in the data files because it is the unique identifier between MyEnroll and the insurance carriers' system.

   FDIC Human Resources retrieve employees' data by performing specific employee searches using either: (1) Name, (2) Social Security, (3) MyEnroll Unique Identifier, or (4) email address.

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.

   FDIC staff members do not run reports from the MyEnroll Report Generator. When reports are needed the FDIC staff members ask BAS representatives to provide them. Reports that are requested may be to determine benefit participation count, eligibility, cost of premiums, problem-solving, etc. BAS provides report information through the SFTP feature and the information is used internally by the FDIC Benefits Staff. These reports are not shared with employees who are outside the FDIC Benefits group.

H. Maintenance and Administrative Controls:

1. If the system is operated in more than one site, how will consistent use of the system, and its data, be maintained in all sites? Will the same controls be used? Explain.

   Not applicable. The system is operated at only one site.

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.

   Records are retained in accordance with National Archives and Records Administration (NARA) Guidance and FDIC Records Retention and Disposition Schedules.

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.

   As noted in Section H.2, records are retained in accordance with NARA Guidance and FDIC Records Retention and Disposition Schedules. Disposal of hard copy reports is by shredding or other means of secure disposal.

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.

   No, the system is not using technologies in ways that the Corporation has not previously employed.

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.

   Not applicable. There is no new use of technology that would affect privacy.

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.

   No monitoring is being performed.

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

   MyEnroll is externally hosted with controls that have been put in place by BAS to prevent unauthorized monitoring. As such, MyEnroll relies on BAS' access controls, firewalls, and intrusion-detection systems to prevent unauthorized monitoring.

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

   This system operates under the following Privacy Act System of Records Notice (SORN): Personnel Benefits and Enrollment Records (30–64–0014)

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

   No. System is not being modified.

I. Business Processes and Technology

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

   No changes to existing business processes are required.

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

   No changes to technology are required.