# 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:** **PEGASYS**

**System Acronym:** **PEGASYS**

**System Owner/Division or Office:** **Michelle Baker-Dubbs, 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.

The system produces a FDIC Identification badge that is used by FDIC personnel and contractors to access the FDIC buildings located in Washington, DC, Arlington, VA, Dallas, Texas, and Memphis, Tennessee. The System allows persons who have been issued a FDIC Identification badge access to FDIC buildings and access to certain restricted areas such as the FDIC Human Resources Branch (HRB), when the badge is scanned by the system's reader pads located at the entrance of the buildings and restricted access areas.

Information stored in PEGASYS is obtained from the FDIC Employee/Contractor Identification Card Request Form (Form 1620/01), which is completed by FDIC employees and contractors. Personnel within the DOA Security Emergency Preparedness Section (DOA SEPS) use the information on the form to populate the PEGASYS database. The PEGASYS database is maintained on an enterprise server located in the FDIC Virginia Square building and connected to the Dallas, Memphis, and Washington, DC offices by a dedicated encrypted virtual private network (VPN).

## 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, Date of Birth, Photo, Height, Weight, Company name, Division, Oversight Manager (OM) (for contractors only) and Badge ID Number on issued badge.

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):

   The Privacy Act Statement displayed on FDIC Form 1620/01 notifies the employee/contractor that the completion of FDIC Form 1620/01 is voluntary. The statement also informs the employee/contractor that failure to provide the requested information may delay or prevent the receipt of an FDIC identification Card.

   ☐ No Explain:

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

   Information stored in PEGASYS is obtained from the FDIC Form 1620/01, which is completed by FDIC employees and contractors. Personnel within DOA SEPS use the information on the form to manually populate the PEGASYS database.

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.

   None

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.

   Only DOA SEPS staff member's assigned responsibility for processing requests for FDIC identification cards will have access to the system. The DOA SEPS staff consists of FDIC employees and contractors. Security Guards who control access to FDIC facilities have limited "view" access to 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 PEGASYS is granted exclusively to employees and contractors assigned to DOA SEPS and the FDIC Security Guards. Access to the system requires management approval and is facilitated and tracked using FDIC's Access Authorization Security Application (AASA).

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

   Access to the data is restricted by privileges assigned to an access type/role. DOA SEPS has full access to the PEGASYS system that allows the users to add, modify and delete data. FDIC Security Guards only have been granted "view" or "read" access, meaning they cannot alter the records in the system in any way.

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 DOA SEPS system administrator produces and reviews audit reports monthly to monitor user actions and to ensure data integrity is maintained.

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.

   No.

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.

   N/A, there is no interface.

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?

   N/A, there is no sharing of the data with other agencies.

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 FDIC Program Manager is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual application users are responsible and accountable for assuring the proper collection and use of the data. Further, the FDIC Program Manager is accountable for establishing the criteria, procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected.

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?

   If privacy related data in the system were intentionally or unintentionally disclosed, it is possible that the FDIC's reputation could be adversely affected.

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?

    PEGASYS is a COTS application maintained by a vendor overseen by DOA SEPS. The vendor provides two individuals, on a full time basis, to support all aspects of PEGASYS for FDIC. The vendor-provided staff has full access to PEGASYS and the data maintained within PEGASYS. The vendor also provides individuals, on an as-needed basis, to support PEGASYS in the Regional and Area offices. The individuals provided by the vendor on an as-needed basis would also have full access to PEGASYS and the data maintained within PEGASYS. Yes, a non-disclosure agreement has been signed.

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.

    N/A

**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.

   N/A

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.

   A limited amount of data fields are populated by data entry personnel. System administrators monitor the system records for completeness.

## 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 data stored in PEGASYS is both relevant and necessary for the purpose of issuing a FDIC Identification Card.

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.

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

   No.

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.

   N/A, the 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.

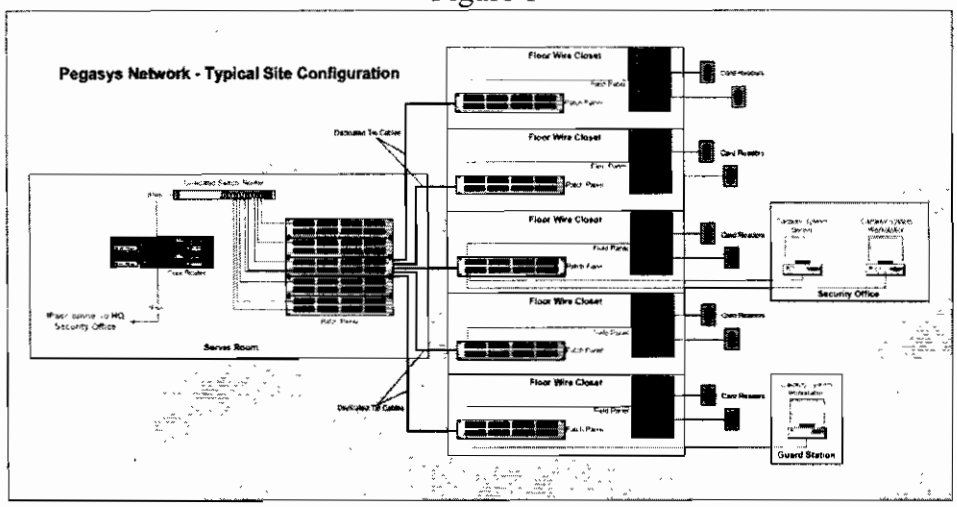
   Data may be retrieved by any data field within the application; therefore, data may be retrieved by personal identifier.

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.

   There are three types of reports produced on individuals by DOA SEPS:

   1. Transaction report – This report is produced monthly, and identifies, by badge reader, the individuals that have gained admission to a badge-reader-controlled entryway during the preceding month.

Figure 1




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 retention period of the data in the system for FDIC employees is five years. The retention period of the data in this system for FDIC contractors is three years. Data will be kept in the active databases for the duration of their employment/contract with the FDIC. When the employee or contractor leaves FDIC, the data pertaining to them will be archived. The retention periods are determined by DOA.

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 long as an individual is employed by the FDIC, or under contract with the FDIC, their information will be maintained in the database. When the employee or contractor leaves FDIC, data will be archived. The retention period of the data in the system for FDIC employees is five years. The retention period of the data in this system for FDIC contractors is three years.

   All reports are produced electronically and are required to be deleted once their intended use has been met. Any paper or electronic media versions of the reports are disposed of using secure shred bins.

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.

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.

   N/A

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.

   Monitoring of individuals is not being performed.

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

   Access to PEGASYS is restricted to DOA SEPS personnel and FDIC Security Guards that have been authorized. The system is located on the FDIC network, and, as such, relies on FDIC Windows General Support System 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.

   FDIC Personnel Records 30-64-0015
   OPM/GOVT-1

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?

   No.

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

   No.