



## **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 A7097.

**Agency:** Federal Deposit Insurance Corporation (FDIC)

**System Name:** **Position Description Update Questionnaire**

**System Acronym:** **HR-PDQ**

**System Owner/Division or Office:** **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 Position Description Update Questionnaire is a mechanism used to collect information from FDIC employees in order to verify the accuracy of the major duties outlined in their position description, as well as to verify their exemption status with respect to the Fair Labor Standards Act (FLSA). Responding to the questionnaire is voluntary on the part of FDIC employees.

The Position Description Update Questionnaire will be conducted by an FDIC vendor. The exchange of information between FDIC Human Resources (HR) and the vendor will be conducted via email using an FDIC-supported FIPS 140-2 compliant encryption product. The information exchanged between the FDIC and the vendor will include: employee name, payplan, series, jobcode, title, division, supervisor name, FDIC employee email addresses, information associated with FDIC employee Position Descriptions, and the FLSA Exemption Status of FDIC employees.

The vendor will collect information related to FDIC employee Position Descriptions and FLSA Exemption Status' directly from FDIC employees using an SSL web-based questionnaire.

The vendor will subsequently prepare and distribute an unencrypted email to the FDIC supervisors of FDIC employees that have completed the questionnaire: The email will contain:

- an external link to the vendor's site, via an SSL connection, to a report that provides a summary of the responses received from the direct reports of the supervisor
- an internal FDIC link to the position descriptions for each of the employees they supervise.
- an external link to the vendor's site, via an SSL connection, to a report that includes the employee's comments, if any, pulled from their questionnaires. The supervisor may add their own comments to the Excel report.

The email will also contain a logon ID and passwords that will be necessary for the supervisor to access the report and links described above.

The vendor will store and safeguard information obtained from FDIC and FDIC employees in accord with the security requirements stipulated in the contract between the FDIC and the vendor.

FDIC HR will store information related to the questionnaire and report(s) in a shared folder on a DIT-supported server with access restricted to only those having a business need to access the information.

#### **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.

FDIC employee names, FDIC employee Position Descriptions and FLSA Exemption Status will be contained within the questionnaire-related data. Additionally, FDIC employees will be able to provide comments and edits related to their Position Descriptions and make recommendations as to how their Position Descriptions should be modified/updated.

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): Participation in the Position Description Update Questionnaire is completely voluntary on the part of FDIC employees. The Privacy Act Statement appearing on the questionnaire will advise FDIC employees of such. However, employees are told that non-participation indicates agreement with their position description.

No Explain:

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

The information used to initiate the questionnaire process will be downloaded from the CHRIS HR application by HR personnel. That information will eventually be combined with information collected directly from FDIC employees, which will subsequently be maintained in an Excel spreadsheet located at the vendor's site.

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.

The Position Description Update Questionnaire will be conducted by an FDIC vendor. The vendor will collect information related to FDIC employee Position Descriptions directly from FDIC employees using an SSL web-based questionnaire. The information collected will be forwarded to FDIC via email using an FDIC-supported FIPS 140-2 compliant encryption product. The information exchanged between the FDIC and the vendor will include: employee names, FDIC employee email addresses, information associated with FDIC employee Position Descriptions, and the FLSA Exemption Status of FDIC employees.

#### **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.

The vendor conducting the Position Description Update Questionnaire on the behalf of FDIC will have access to the data in their role as data collector and evaluator of the position descriptions as they relate to the employees' job responsibilities. Additionally, an employee's supervisor will have access to the data the employee has provided. Further, individuals within DOA HR (including classification and compensation staff) that have a business need will also have access to the data, as will panel subject matter experts and, potentially, members of the FDIC's Legal Division.

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 Position Description Questionnaire data will be role-based and restricted to those having a business need. Appropriate management level approval will be required for all access.

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

Access to the Position Description Questionnaire data will be role-based and restricted to those having a business need.

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.

All DOA HR employees must meet the requirements for securing confidential business data and personally identifiable information as outlined in the FDIC's Corporate Information Security Awareness Training course and Privacy Act Awareness Training course. Both courses must be completed by FDIC employees on an annual basis. Additionally, users of the questionnaire data are required to comply with FDIC Circular 1360.9 - *Protecting Sensitive Information*.

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

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

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 Program Manager responsible for the Position Description Update Questionnaire, as well as HR Compensation Staff and HR Classification Staff, is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual users of the questionnaire data are responsible and accountable for assuring that they are properly using the data. The

Position Description Update Questionnaire Program Manager has overall responsibility for the questionnaire data and 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 associated with the questionnaire were intentionally or unintentionally disclosed, it is possible that it would cause embarrassment for the FDIC.

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 Position Description Update Questionnaire will be conducted by a contractor. The contractor will collect information related to the FDIC Position Description Update Questionnaire from FDIC employees and exchange that information and other related information with FDIC HR staff. In accord with the contract between FDIC and the contractor, a Non-Disclosure Agreement has been completed by the contractor.

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 data owner would be notified in the event of a data breach, per FDIC data breach procedures. The contractor is contractually required to immediately report all security and privacy incidents that impact, or may impact, FDIC information/data to FDIC's Computer Security Incident Response Team (CSIRT).

## **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.

The data collected from sources other than FDIC records will be verified and validated for accuracy by employees' supervisors and/or the HR staff responsible for processing the questionnaire results.

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.

The data collected from sources other than FDIC records will be verified and validated for completeness by employees' supervisors and/or HR staff responsible for processing the questionnaire results.

### **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.

All of the data collected is relevant and necessary to the purpose for which the questionnaire is designed.

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.

It is not intended for additional Personally Identifiable Information to be derived from the aggregation of the questionnaire results. Additional Personally Identifiable Information could be derived, however, based on the proposed comments/edits collected by FDIC employees completing the questionnaire. Users of the questionnaire data, through reviewing the collected information would have to make this determination. The determination would be based on the judgment of the user.

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

It is not intended for additional Personally Identifiable Information to be derived from the aggregation of the questionnaire results. Users of the questionnaire data, through reviewing the collected information would have to make this determination. The determination would be based on the judgment of the user.

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.

See Section E. Access to Data, for the controls on access to the Position Description Update questionnaire data.

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.

Questionnaire data can be retrieved by FDIC Employee name.

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 reports will be prepared to ensure the appropriate processing of questionnaire results. The distribution of such reports will be restricted to those individuals having a legitimate business need.

#### **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.

Summaries of employee comments will be housed on the Vendor's site, and accessed by the appropriate supervisors for review. The supervisor will be sent a password, via email, ensuring that only the supervisor can review his/her employees' comments. DOA HR will also have access to the summaries, if necessary, for the review.

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 information related to the Position Description Update Questionnaire will be retained in accord with FDIC's Records Retention 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.

The information related to the Position Description Update Questionnaire will be disposed of in accord with FDIC's Records Retention Schedules.



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 is not being performed.

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

The questionnaire data will only be accessible to those contractors and FDIC employees having a legitimate business need. The questionnaire data that is located on the FDIC network will rely on FDIC Windows General Support system access controls, firewalls, and intrusion-detection systems to prevent unauthorized monitoring. With respect to the questionnaire data that may be maintained at the contractor site, the contractor is contractually required to implement reasonable administrative, technical, physical and procedural security and privacy controls to ensure that all FDIC information/data in their possession or under their control is protected from loss, misuse, and unauthorized access or modification. Further, the contractor is required to ensure that the collection, use, transmission, and disclosure of FDIC information/data is in compliance with all federal and state privacy laws and FDIC rules and regulations regarding privacy.

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

30-64-0015 - Personnel Records

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.