FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

For

Office of Inspector General (OIG) Training and Professional Development System (TPDS)

Date Approved by Chief Privacy Officer (CPO)/Designee
4/10/2019

Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

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.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

The Training and Professional Development System (TPDS) release 1.0 will be an automated information system that tracks, reports, and processes personnel training requests in the Federal Deposit Insurance Corporation (FDIC) – Office of Inspector General (OIG). TPDS will store FDIC OIG employee and supervisor full names, training vendor information, and training course information. Such training-related information may assist OIG employees and management in planning future training and tracking compliance with any applicable continuing education requirements. Additionally, TPDS will be used by the OIG to track and report on continuing professional education requirements (CPE) for OIG staff. TPDS will present a security and privacy sign-on banner requiring acknowledgement by authorized users.

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

TPDS collects, uses, and maintains the full names of employees, supervisors, management, vendor points of contact, and employee training records. In addition, TPDS will generate a system identifier that will be associated with each FDIC OIG employee that is added as a user to the application. The generated system identifier will be internal to TPDS only.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

PII collected and used in TPDS is required for the core functionality of the application. The full names of employees must be linked to the training records that are processed in the system to ensure requests are routed to the appropriate approving official. In addition, the training records will be maintained in the system to support the tracking and reporting of CPE for OIG staff.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

a) Explain the business purpose/need requiring the collection of SSNs: N/A

b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

☐ Yes List any additional legal authorities: N/A
☐ No

c) Is the SSN is masked or otherwise truncated within the system?

☐ Yes. Explain: N/A
☐ No. Is it possible to mask or otherwise truncate the SSN within the system?
☐ Yes. Explain how it may be masked or truncated and why this has not been implemented: N/A
☐ No. Explain why it may not be masked or truncated: N/A

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

☐ Yes. Explain: N/A
☐ No. Is it possible to restrict access to specific groups of users within the system?
☐ Yes. Explain how access may be restricted and why this has not been implemented: N/A
☐ No. Explain why access cannot be restricted: N/A

3.4 Who/what are the sources of the information in the system? How are they derived?

OIG personnel manually input the records entered, used, and managed in TPDS, which may include training course information obtained from training vendors.

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain. None.

3.6 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.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☒ No Explain:
The use of TPDS is required by OIG Management. The PII collected is necessary to track and appropriately route each training request for supervisory approval or rejection.

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

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 **Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.**

TPDS application users having standard access can only access their own data. Users with a need for privileged access (training coordinators, and administrators) are granted access to all employee training records. Supervisors and Managers have access to training records associated with their subordinate employees. The data stored in TPDS is not accessible to external parties.

4.2 How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access.

All OIG employees are required to have access to TPDS. The FDIC Access Request and Certification System (ARCS) is used to grant, manage and monitor access to TPDS. Access to TPDS is role-based and determined by the employee's job function within the OIG. The roles in TPDS are as follows:

- standard users (employees)
- approvers (supervisors, managers)
- coordinator (OIG personnel responsible for registering and paying for approved training)
- Administrators (OIG personnel who perform system administration functions)

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

☒ No
☐ Yes Explain.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

N/A

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The TPDS System Owner is responsible for assuring proper use of data in the system. Also, it is the responsibility of all individual users to ensure the proper use and protection of corporate data in accordance with FDIC directives and the annual FDIC Information Security and Privacy Awareness Training, which includes guidance and direction on protecting sensitive information and sensitive personally identifiable information.

4.6 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?

No contractor resources have been utilized for the design and maintenance of TPDS.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

Required data fields have input validation checks in place. Training request approvers and training coordinators must also review the data entered by employees prior to processing.

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

Security and access restrictions are in place and enforced on the client and server side to restrict unauthorized access to data stored in TPDS. Each read and write transaction in TPDS is verified for valid authentication information. In addition, authorization controls occur at each transaction using input verification functions and role based permission checks.

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 **How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

Employee training data is retrieved by three distinct methods.

1. Employee name: ex. John Doe

2. Component office acronym: ex.
   OIT - Office of Information Technology
   ITC - Office of Information Technology and Cyber Audits
   PAE - Office of Program Audits and Evaluations
   OI - Office of Investigations
   OM - Office of Management
   OGC - Office of General Counsel
   FO - OIG Front Office

3. Date Range – for example, using Start Date and End Date for filtering the datasets.

6.2 **What kind of reports can be produced *on individuals*? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?**

The Training History report for an individual will be produced by TPDS. The report contains the training events requested by an individual, including associated approval status, and other related information about the training request. The report will be dynamically generated on demand by the user, and will not

be maintained in the system. Additionally, users and approvers may produce reports that identify the number of CPE credits that are associated with each user. Access to reports of an individual's CPE credits is restricted to that individual and their supervisor or manager.

6.3 What are the retention periods of data in this system? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The retention period for data maintained within TPDS is seven years, which is consistent with the FDIC Records and Information Management Unit's (RIMU) record retention schedule for employee training records.

Eligible data will be purged from the system through the administration console, which will identify data residing in the system that exceeds the data retention period.

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

FDIC-30-64-0007 FDIC Learning and Development Records

6.5 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

N/A

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

No.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

No.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

The system maintains only full names of employees, supervisors, management, vendor point of contacts and Employee Training Records. Therefore, the data is categorized at the low impact level. The intentional or unintentional disclosure of this data would not affect the reputation of the Corporation.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

No.