FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

LEGAL

National Employee Ethics Tracking Systems II

(NEETS II)

Date Approved by Chief Privacy Officer (CPO)/Designee

August 5, 2013

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 FDIC Legal Division's Ethics Unit (EU) oversees ethics training and disclosure compliance for current and former FDIC officers and employees, and special government employees. To this end, the Ethics Unit staff uses the National Employee Ethics Tracking System (NEETS II) to electronically assign and track FDIC employees'

[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..

completion of required U.S. Office of Government (OGE) public financial disclosure reports and related FDIC Employee Ethics Disclosure Forms. NEETS II automates the ethics filing process, eliminating cumbersome, manual processing and encouraging timely compliance with applicable Federal conflict of interest laws and regulations. In addition, NEETS II is used to track employees' completion of live and online FDIC ethics training courses.

NEETS II automatically assigns the appropriate ethics forms to FDIC employees based on their assignment, grade and other ethics filing rules. NEET II generates emails to employees notifying them of the filing requirement. Employees then use the system to complete and submit the forms electronically to the FDIC Ethics Unit. E-Level filers are also required to file periodic transaction report if the amount of transaction for stocks, bonds, commodity futures and other securities exceeded $1000. The forms are reviewed by Deputy Ethics Counselors (DECs), who are persons within each FDIC division trained by the Ethics Unit to review the various forms, and by Senior Ethics Program Specialists in the FDIC Ethics Unit. Rejected forms can be sent back to the employee to be updated or corrected as needed. The completed and approved forms are retained in NEETS II.

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.

The following information is contained in NEETS II:

- Employee Name;
- Employee Identification Number;
- Employment Status;
- Home Address;
- Work Phone Number;
- Listing and Dates of Annual FDIC Ethics Training and Forms Completed/Not Completed by Employee (e.g., includes listing and status of required forms or training).

In addition, the Ethics Forms maintained within NEETS II contain the following information:

- Personal Financial Data (e.g., information regarding an employee's financial interest in FDIC-insured depository institution securities; any non-credit card financial obligations owed to FDIC-insured depository institution and/or its subsidiary; and any other reportable assets, income, and liabilities, agreements and arrangements); and
- Other Data Pertaining to Outside Work Activities (e.g., positions held by FDIC employees outside of the U.S. Government, gifts/travel reimbursements received by the employee, and other outside agreements/arrangements)

Note: Public Financial Disclosure Reports (OGE Form 278) and Periodic Transaction Report (OGE Form 278 T) completed by certain FDIC employees are available for public inspection by submitting a formal written request to the Ethics Unit, which includes the requester's name, occupation, address, and a description of the reports requested. Responses to requests typically involve sending a copy of the form by mail. Requests are received in hard copy format and stored in a locked file room by Ethics Unit staff. Requester information is not entered into NEETS II.

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

The information contained in NEETS II is necessary in order to ensure compliance with applicable Federal conflict of interest laws and regulations.

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

(1) **Employee Ethics Forms:** The information in the system consists of various ethics disclosure forms completed by individual FDIC employees or a person or entity designated by the individual. These forms include OGE Form 450, *Confidential Financial Disclosure Report;* OGE Form 278, *Periodic Transaction Report;* OGE Form 278T, *Public Financial Disclosure Report;* Form FDIC 2410/06, *Confidential Report of Indebtedness;* Form FDIC 2410/07, *Confidential Report of Interest in FDIC-Insured Depository Institution Securities;* and Form FDIC 2410/09, *Employee Certification and Acknowledgement of Standards of Conduct Regulation.*

The following describes the specific data elements collected on each form:

- Employee Full Name (Form FDIC 2410/06, Form FDIC 2410/07, Form FDIC 2410/09, OGE Form 450, and OGE Form 278).
- Employee Identification Number (Form FDIC 2410/06, Form FDIC 2410/07, and Form FDIC 2410/09).
- Employee Phone Number (Office) (Form FDIC 2410/06, Form FDIC 2410/07, Form FDIC 2410/09, and OGE Form 278, and OGE Form 450).
- Employee Financial Information (Form FDIC 2410/06, Form FDIC 2410/07, OGE Form 450, OGE Form 278 and OGE 278T).
- Employment Status (Form FDIC 2410/06, Form FDIC 2410/07, Form FDIC 2410/09, OGE Form 450 and OGE Form 278).
- Other Data Pertaining to Outside Work Activities (OGE Form 450 and OGE Form 278).

(2) Employee Ethics Training Data: FDIC Ethics Unit staff manually enters training data into NEETS II based on lists of individuals completing live or computer based ethics training.

(3) FDIC Corporate Human Resources Information System (CHRIS): The CHRIS HR system provides a limited feed of data for administrative contact purposes, as well as, to appropriately assign and route required ethics forms to FDIC employees for completion. PII collected from CHRIS includes:

- Employee Name;
- Employee Identification Number;
- Home Address;
- Employment date of appointment and Status.

3.4 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.

Data is not provided by Federal agencies for use in the system

3.5 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.

Data is not provided by third party sources for use in the system.

3.6 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)?

☐ 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:

There is no opt-out option for individuals. The information contained in NEETS II is necessary in order to ensure compliance with applicable Federal conflict of interest laws and regulations.

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.

Explain who will have access to the data in the system, including both internal and external parties, such as managers, system administrators, system users, contractors, developers, etc. Also consider "other" users who may not be as obvious, such as the Government Accountability Office (GAO) or the Office of Inspector General (OIG). Additionally, if applicable, include the parties listed in the Privacy Act System of Records Notice (SORN) under the "Routine Use" section when a Privacy Act SORN is required.

For each category of users, explain their purpose for access. A user should be given access to data only on a "need-to-know" basis for information required to perform an official function. Care should be given to avoid "open systems" where all of the information can be viewed by all users. System administrators may be afforded access; however, access should be restricted when users do not need to have access to all of the data.

The following internal FDIC users will have access to NEETS II:

- **FDIC Employees**: All FDIC employees have limited access to NEETS II to complete, review and file their own ethics forms. Each employee has access only to his/her respective ethics forms.

- **FDIC Ethics Unit Staff/Administrators & Reviewers:** Authorized staff in the FDIC Ethics Unit will have administrator access to all data in the system. The purpose for their access is to maintain the system, review completed ethics forms for accuracy, notify employees of any updates/corrections that need to be made to the forms, approve forms, and run reports to track compliance/completion of ethics forms and training by employees.

- **FDIC Deputy Ethics Counselors (DECs)/Reviewers**: There are approximately 70+ DECs with access to the system. DECs are designated regional representatives from each FDIC Division/Office who are trained and authorized by the Ethics Unit to review the various ethics/financial disclosure forms under their respective purview for compliance with applicable ethics laws and regulations. A DEC's access to the system is limited; he/she is only able to review the ethics forms of employees in his/her respective Division or Office, unless it is deemed necessary by the Ethics Unit NEETS II Program Manager for a DEC to review other ethics forms as part of his/her business functions.

- **OGE, Government Accountability Office (GAO) and US Department of Justice Employees**: In addition to the aforementioned internal users, on occasion, OGE and GAO staff may review a selection of the ethics forms on a random schedule to ensure compliance with the government ethics statutes and regulations. Also, DOJ staff may have access to the records when the use of such records is deemed relevant and necessary to assist with investigations or litigation involving those records. These routine uses are covered in the FDIC System of Records Notice (SORN) for NEETS II (i.e. 30-64-0006, Employee Confidential Financial Disclosure Records), as well as the following OGE SORNs: OGE/GOVT I, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, and OGE/GOVT2, Executive Branch Confidential Financial Disclosure Reports.

- **Members of the Public**: The FDIC is required to share publicly available financial disclosure information contained in NEETS II with members of the public and other external agencies when a formal request is made using OGE Form 201, Request to Inspect or Receive Copies of Form 278 Executive Branch Personnel Public Financial Disclosure Reports or Other Covered Records. Upon receiving such a request, the forms are sent to OGE via email or mail by the applicable NEETS II Ethics Program Manager or the form may be sent directly to the requester via mail.

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

- Access to data is determined by the Ethics Program Manager/Data Owner for NEETS II based on a person's business requirements and granted on a "need to know" basis, as described in Section 4.1.

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.

There are no interfaces between NEETS II and external systems. However, in terms of internal connectivity, NEETS II receives data from FDIC's Corporate Human Resources Information System (CHRIS), as described in Section 3.3. The data collected from CHRIS includes Employee Name, Home Address, Employee Identification Number, and Employment Status. This data is necessary for administrative contact purposes and to appropriately assign and route applicable ethics forms to the right employees.

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.

As noted in Section 3.4, FDIC does not share information with other agencies unless a formal request has been made with the Office of Government Ethics (OGE) using Form 201, "*Request to Inspect or Receive Copies of Form 278 Executive Branch Personnel Public Financial Disclosure Reports or Other Covered Records"*. Upon receiving such a request, the forms are sent to the Office of Government Ethics via email by the applicable NEETS II Ethics Program Manager. This is the specified procedure for all individuals and agencies.

In addition, OGE and the Government Accountability Office (GAO) may review a selection of the ethics forms on a random schedule to ensure compliance with the government ethics statues and regulations. Also, on occasion, Department of Justice employees may have access to the records when the use of such records is deemed relevant and necessary to assist with investigations or litigation involving those records. These routine uses are covered in the FDIC System of Records Notice (SORN) for NEETS II

(i.e. 30-64-0006, *Employee Confidential Financial Disclosure Records*), as well as the following OGE SORNs: OGE/GOVT 1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records*, and OGE/GOVT2, *Executive Branch Confidential Financial Disclosure Reports.*

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 Ethics Program Manager/Data Owner and Legal Division Information Security Manager (ISM) serve as the primary sources of information for data definition and data protection requirements for NEETS II. They are collectively responsible for supporting a corporate-wide view of data sharing. Although they share this data responsibility, it is every user's responsibility to abide by FDIC data protection rules that are outlined in the Corporate Security Awareness Training and Privacy Act Awareness Orientation, which all employees take and certify they will abide by the Corporation's Rules of Behavior for data protection. This makes it the responsibility of every user to ensure the proper use of corporate data.

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?

FDIC worked with a contractor to design and develop the system and contractors may be employed to provide support and maintenance for this system. Each contractor with access to NEETS II data is required to sign a Contractor Confidentiality Agreement and Non-Disclosure Agreement and complete FDIC's Corporate Security Training and Privacy Orientation, which includes Rules of Behavior.

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?

FDIC employees are responsible for ensuring that the information they provide on an ethics form is complete and accurate. Also, all ethics forms go through a review process by FDIC DECs and FDIC Senior Ethics Program Specialists, so completeness of data is determined by the Reviewer.

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

- Access to data is determined by the Ethics Program Manager/Data Owner for NEETS II based on a person's business requirements and granted on a "need-to-know" basis, as described in Section 4.1.
- User's access is restricted by the Ethics Program Manager/Data Owner for NEETS II based on role-based access controls and their "need-to-know", as described in Section 4.1.
- Authorized FDIC Ethics Unit administrator can execute Audit Reports –"User profile change report" and "system settings change reports" to monitor and ensure there is no authorized access.
- NEETS II will use the standard Pega Authorization Model coupled with Lightweight Directory Access Protocol (LDAP) external authentication. LDAP is a software protocol that helps manage information

about a system's authorized users and their data access privileges. Roles (i.e. Pega Access Groups) will be set up for standard users (Filers) as well as administrators (Reviewers). Therefore, users will only have access to the data they are authorized to view, as required.

- Additionally, a Corporate Security Awareness Training and Privacy Act Awareness Orientation, which includes the Rules of Behavior is mandated for all users in the FDIC network. This training has specific information regarding the compromise and prevention of misuse of data. FDIC users are required to undertake these awareness training programs annually.

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.

Authorized NEETS II DECs and Senior Ethics Program Specialists can retrieve data on an employee by searching by Employee Name, Account Name or Employee Identification Number.

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?

Authorized staff in the FDIC Ethics Unit may run reports, as needed, to determine whether or not employees have completed their mandatory ethics forms and training, as well as to send reminders to those who have not completed the required forms and training. Authorized FDIC Ethics Unit administrator can execute Audit Reports –"User profile change report" and "system settings change reports" for audit management. These reports are used strictly for the aforementioned compliance tracking purposes.

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.

Ethics Unit staff follows the guidance in the Records Retention and Disposition Schedule published by the FDIC Division of Administration for data contained in NEETS II. Records are retained for six years and then destroyed. Electronic or paper documents needed for an ongoing investigation will be retained until no longer needed for that investigation.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with National Archives and Records Administration (NARA) guidance. For NEETS II, the procedure typically is disposal is by shredding or other appropriate disposal systems.

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

The system operates under the following FDIC Privacy Act System of Records Notice: "30-64-0006, Employee Confidential Financial Disclosure Records." For a listing of current FDIC Privacy Act Systems of Records, please visit: http://www.fdic.gov/regulations/laws/rules/2000-4000.html.

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

No amendments' or revisions to SORN are required.

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
☐ Yes Explain:

No, the data is not being consolidated and the system will not derive any personal identifiable information from new data that was previously non-inclusive. All personal identifiable information is received from CHRIS HR and user input.

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.

Not applicable. There is no new use of technology that would affect privacy. The system does not use technology in ways that the Corporation has not previously employed.

7.3 Will the system 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.

Not applicable. Monitoring is not being performed. The system implements role-based access control to prevent against unauthorized monitoring.

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?

NEETS II contains personally identifiable information about FDIC employees, such as name, home address, employee identification number, and financial disclosure information. In light of the information contained in the system, the loss of confidentiality is deemed to be a moderate risk and could have an adverse effect on the organization's reputation. Additionally, since the system contains personal information about FDIC employees, it is necessary to maintain safeguards against the potential of fraud or theft by either FDIC employees or persons outside the Corporation. Disclosure of this data could be harmful to both individuals and the Corporation. Therefore, FDIC takes all security measures necessary to prevent an unauthorized disclosure.

7.5 Did the completion of this PIA result in changes to business processes or technology?

☒ No
☐ Yes Explain:

No changes to business processes are required.