FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Division of Administration (DOA)

WebTA

Date Approved by Chief Privacy Officer (CPO)/Designee:
12/18/2017

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.

WebTA (formerly known as the "Corporate Time and Attendance System" or "CHRISTA") is a web-based, FDIC-customized version of the commercial-off-the-shelf Time and Attendance software application from Kronos. It provides the Corporation with an integrated time and attendance system that provides accurate, timely and efficient reporting of time and attendance (T&A) data for all FDIC employees and supports the collection of corporate cost management data for New Financial Environment (NFE)[3]. In addition, it provides the following functionality:

- Managing time and attendance reporting, validation, and certification for all FDIC employees.
- Providing a single view into all employee data, including timesheets, leave requests and balances, and profile information.

[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.

[3] *See* NFE PIA.

- Allowing employees to submit and approve leave requests online and automatically transmit data to accrual balances and timecards.
- Interfacing time and attendance data with the National Finance Center (NFC).
- Interfacing accounting data with NFE.
- Interfacing activity data with Divisional reporting systems such as Advanced Legal Information System (ALIS)[4], DSC Hours[5], and New Financial Environment - Payroll Transmission Accounting and Reporting (NFE-PTAR)[6].

WebTA also allows FDIC employees, timekeepers, and supervisors to:

- Fill out a timesheet for a future pay period (one pay period ahead);
- View future leave balances;
- Receive reminders when comp time or time-off awards are about to expire;
- Submit and track telework requests more easily; and,
- Track the status of timesheet approvals and leave requests.

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 system contains personal information about FDIC employees including their full names, Social Security Numbers (SSNs), Employee Identification Numbers (EINs), Network IDs (NTIDs), and work email addresses. The system also contains employee work schedules; pay plans; timesheets; telework, premium pay, and leave requests and balances; and employee and supervisor remarks/comments related to employee leave, premimum pay and telework requests (e.g., purpose for taking the leave, projects to be completed while teleworking or working extra hours, justification for denying the leave request, etc.).

Note: Any documentation that may be required to support employee leave requests (e.g., doctor notes, Family Medical Leave Act paperwork, etc.) is not uploaded to or maintained in WebTA. Generally, this information is maintained by the employee's supervisor in hard copy. However, the employee may enter references to this documentation in the remarks/comments section of their leave request in WebTA.

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

The information described in Question 3.1 is used to facilitate and manage FDIC employees' time and attendance reporting, and validation and certification, as well as provide views of employee data including timesheets; leave, premium pay, and telework requests and balances; and profile information. The employee's name, SSN, and time and attendance data are securely passed to the United States Department of Agriculture (USDA) National Finance Center (NFC) system for payroll processing. NFC requires SSN as an employee identifier to complete its processing.

In addition, the data elements in Section 3.1 are required to manage and complete internal time and attendance transactions for FDIC employees; interface accounting data with NFE-PTAR to update the general ledger; and interface activity data with various internal systems (specified in Section 4.3) to support Divisional reporting and timekeeping activities.

[4] *See* ALIS PIA.
[5] *See* DSC Hours PIA.
[6] *See* NFE PIA.

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: SSNs are required for employee payroll processing by NFC, including tax reporting to governmental agencies. As stated in question 3.3 (c) the SSN is masked for all WebTA users except Human Resources Branch (HRB) Administrators. Analysis is done for feeder systems to determine if the SSN is required; otherwise, it is excluded or encrypted in the feed. The SSN is used to interface with NFC since it is the common and unique identifier between WebTA and NFC . NFC returns data based on SSN, and NFE-PTAR uses the SSN to match data with WebTA to generate payroll transactions at the required data detail level.

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: 26 U.S.C § 6109(a)(1)(d): Any person required to make a [IRS] tax return, statement, or other document with respect to another person shall include the social security account number issued to such person for purposes of section 205(c)(2)(A) of the Social Security Act, as the identifying number for such person.

☐ No

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

☒ Yes. Explain: SSN is masked for all users except for the HRB Administrators.

☐ 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:

☐ No. Explain why it may not be masked or truncated:

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

☒ Yes. Explain: Only authorized DOA HRB Administrators can see the SSN. The SSN is masked for all other users.

☐ 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:

☐ No. Explain why access cannot be restricted:

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

Information is manually entered into the system by the individual employee, supervisor, authorized Divisional timekeepers, and DOA HR staff. In addition, the system imports information from the following FDIC systems:

System	Connection Method	Description of Data Imported
Advanced Legal Information System (ALIS)	Batch processes	WebTA obtains account cross-reference data for legal matter accounts from ALIS via batch processes. This data is used to help track time charged to specific legal matters. No PII is included.
Corporate Human Resources Information System (CHRIS)	Batch processes	In order to reduce the amount of redundant data and support seamless operation of FDIC systems, WebTA extracts employee data, including full name, work email address, NTID, EIN, SSN, Personnel Officer Identifier (POI), department ID, grade and pay plan, teleworking eligibility, and organization tree information, from CHRIS via batch processes.
DSC Hours	Batch processes	WebTA obtains account cross-reference information for exam and application accounts (i.e., exam/project numbers) from DSC Hours in order to charge time against financial institution (FI) exam and project activities. No PII is included.
Manual Entry by FDIC Employees	Manual Entry	FDIC employees enter their own leave, premium pay, and telework requests in WebTA, validate and affirm their own timesheets, and maintain their own person accounts and default schedules. In the Comment fields, employees may enter

		information/justification (which may be personal in nature) for their telework, leave, and premium pay requests.
New Financial Environment Interface Operational Data Store (NFE IODs)	Batch processes	NFE IODs sends FDIC chart fields, codes and corporate cost accounting data used to create reporting account codes to WebTA for account building. This information is essential for employees to build their timesheets. No PII is included.

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.

No Federal, state, or local agencies provide data for use in WebTA.

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.

No other third-party sources will be providing data for use in WebTA.

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 PII collected is required as a feed into the NFC system for payroll processing. NFC applications rely heavily on the SSN for validation in order to complete their processing.
☐ 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.
The following parties are authorized to have access to the system for the purposes outlined below:

FDIC Employees have access to their own T&A information. They enter their own leave, premium pay, and telework requests in WebTA, validate and affirm their own timesheets, and maintain their own personal accounts and default schedules.

FDIC Supervisors review the T&As submitted by their employees to ensure that they are correct, certify the T&As submitted by their employees, review and approve electronic leave and premium pay requests, ensure that their employees enter the appropriate Cost Management information, maintain medical and other confidential documentation outside of the system, and may serve as the delegate for other Supervisors.

FDIC Timekeepers complete New Employee Set-Up & maintain Employee T&A Profiles (contact point, work schedule, etc.) throughout the employment cycle. They assist employees by maintaining frequently used cost management information in T&A "Accounts" and help employees to set up and maintain personal accounts and default schedules. Timekeepers help employees enter their time properly, assist supervisors in reviewing leave requests prior to approval, and provide a quality control checkpoint prior to supervisor approval of T&As. They enter T&A corrections, help some employees to enter correct T&As, and enter time and validate T&As for employees who are unable to do so. Any FDIC employee may serve as a timekeeper if so assigned by his/her organization.

FDIC HR Administrators within DOA serve as the POCs for all T&A issues within their respective regions. They train new timekeepers and serve as "Master Timekeeper" for the region. They set up, maintain, and close out Leave Transfer Program (LTP) cases. HR Administrators review the status of T&A records within the region, give employees control over their timesheet corrections through the employee profile page, reconcile WebTA with NFC and resolve rejected timesheets, and oversee or process split T&As.

FDIC Administrators within DOA have the highest level of access available in WebTA. Administrators maintain system configuration information and monitor the biweekly build process.

Auditors have read-only access to T&A records for all FDIC employees on a need-to-know basis. Access to SSN is not included.

Executive Self-Certification access in WebTA gives the user the ability to certify his/her own T&A. This access is currently restricted to one (1) person within the Executive Office.

Note: Contractors do not have access to WebTA. WebTA is for use by FDIC employees only.

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

Access requests to data and functionality in WebTA is based on user role. FDIC employees are automatically granted access to WebTA through an interface with CHRIS. Exceptions are manually provisioned by HR. This will give an employee access to their own data – timesheets and requests for leave, premium pay, and telework.

An approved Access Request and Certification System (ARCS) request is required for any access other than active FDIC employee. Aprroval by the employee's supervisor and the data owner is needed before the access is granted.

The HR Administrator, FDIC Administrator, Auditor, and Executive Self-Certification roles are highly restricted based on the user's job requirements and managerial decisions.

See question 4.1 for more information on the WebTA functionality assigned to each role. Documentation for obtaining access to WebTA is available on the DOA web page on the FDIC Intranet.

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.

WebTA exports data to the following FDIC systems:

System	Connection Method	Description of Data Exported
Advanced Legal Information System (ALIS)	Batch processes	WebTA sends employee time and attendance (TA) transactions to ALIS via batch processes for purposes of tracking time charged to specific legal matters. Specific data elements shared include the hours per EIN charged to a particular legal matter account code.
Corporate Human Resources Information System (CHRIS)	Batch Job	WebTA sends employee timesheet and leave balance information, which includes PII, to CHRIS for reporting purposes. This interface facilitates the querying of both CHRIS and WebTA data in the same database for ease of use.
DSC HOURS	Batch processes	WebTA sends employee time and attendance (TA) data via batch processes to DSC HOURS for tracking time

		charged to a financial institution (FI) application or exam-related activities. Specific data elements shared include account codes, employee user NTIDs, and their timesheet charges for the most recent pay period
Enterprise Data Warehouse (EDW) /FDIC Data Marts	Batch processes	WebTA shares employee timesheet data via batch processes with FDIC EDW and various FDIC Data Marts, such as the Strategic Workforce Planning Initiative (SWPI)/Recruitment Activity Process Tracking (RAPT) System in support of tracking recruitment activity for FDIC; the Reporting Data Mart Migration (RDMM) in support of FDIC regional office and Corporate headquarters reporting and analysis efforts; and the Human Capital Management Data Mart (HCMDM) in support of corporate strategic workforce planning, tactical human capital management, and decision-making at all levels within FDIC.
New Financial Environment - Payroll Transmission Accounting and Reporting (NFE-PTAR)	Manual download and sent via Entrust [7]	WebTA sends chartfield data (i.e., account code division reference and exam type which does not include PII), as well employee T&A and leave data (i.e., a copy of data sent to the National Finance Center) to ensure wages paid to employees are properly recorded on the general ledger. This data includes employee name, SSN, and timesheet charges for the most recent pay period.

WebTA exports data to the following external systems:

Name of Entity	Connection Method	Description of Data Exported
NFC	Secure File Transfer Protocol (SFTP)[8]	Employee time and attendance (T&A) and leave data are shared with NFC. This data includes employee name, SSN, and timesheet charges for the most recent pay period.

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.

Access will be provided only to those parties identified in the routine use section of the Privacy Act System of Records (30-64-0015, *Personnel Records* [80 FR 67001]).

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 WebTA Program Manager/Data Owner is responsible for assuring proper use and integrity of the data. The WebTA Program Manager/Data Owner and DOA Information Security Manager also serve as the sources of information for data definition and data protection requirements. Although they share this

[7] The time and attendance data build file is sent via secure ftp from WebTA to the NFC mainframe three times a week on payroll weeks. NFC processes the build file when running FDIC's payroll. The same build files are sent from WebTA to an internal FDIC ftp server for processing by the NFE-PTAR application. The WebTA build files are sent manually by HRB Administrators via encrypted email to DOF NSCS Operations for processing into NFE-PTAR. NSCS Operations will manually load the WebTA files on the secure ftp server for NFE-PTAR. An automated solution is being worked on to resolve an issue with the file structure. Implementation of the automated solution is to be determined.

[8] The time and attendance data build file is sent via secure ftp from WebTA to the NFC mainframe three times a week on payroll weeks. NFC processes the build file when running FDIC's payroll. The same build files are sent from WebTA to an internal FDIC ftp server for processing by the NFE-PTAR application. The WebTA build files are sent manually by HRB Administrators via encrypted email to DOF NSCS Operations for processing into NFE-PTAR. NSCS Operations will manually load the WebTA files on the secure ftp server for NFE-PTAR. An automated solution is being worked on to resolve an issue with the file structure. Implementation of the automated solution is TBD.

data responsibility, all system users are responsible for abiding by FDIC data protection rules that are outlined in the Corporate Information Security and Privacy Awareness training which all employees must take and certify that 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?

Contractors have served as the main source for design and maintenance tasks. Contractor Confidentiality Agreements/Non-Disclosure Agreements have been signed.

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?

The system is designed to require that specific information is entered for each transaction in order for it to be complete. If the required information is not entered, the time and attendance transaction will not be accepted by WebTA. Individuals provide their own time and attendance information, and are able to view their own information, so they are able to access and correct this information as necessary.

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

Administrative controls include annual and quarterly reviews of user access by the WebTA system administrators. The annual reconciliation is done for users with elevated WebTA access (more than active employee) by comparing access control information from ARCS with user role information in WebTA. A reconciliation spreadsheet is used to ensure that every current WebTA user has an appropriate corresponding ARCS access level. Any WebTA roles inconsistent with ARCS access levels will be removed, except for those in which a user with Supervisor or Timekeeper Access in WebTA has employees assigned to them in WebTA. In such cases, the user's supervisor and Administrative Officer will be contacted either (1) to reassign the employees to a different Supervisor/Timekeeper so that the access can be removed in WebTA or (2) to submit a new ARCS request for the access to ensure reconciliation between the two systems.

The system contains security controls that protect the WebTA application from unauthorized access. Access to WebTA is granted only to those persons within the FDIC specifically authorized by the Corporation. Access levels and permission levels have been established and access provided only to those persons who have a need to know the information contained in the system in order to carry out their duties. In accordance with Federal regulation, law and policy, WebTA has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

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.

Data may be retrieved by EIN (EMPLID), WebTA EIN, NTID, SSN and/or full name, depending upon user

role and WebTA function.

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 system produces reports using various parameters determined by the user but limited to only the information for which the user has access, based on his or her "need to know." DOA is working with Records and Information Management (RIM) group to establish a retention schedule.

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 Payroll/Timekeeping and Time and Attendance data/records is seven (7) years per FDIC records retention schedule code PER4200. This includes all time and attendance records upon which leave input data is based, such as timesheets; time cards (such as Optional Form OF-1130); flextime records; leave applications for jury and military duty; and authorized premium pay or overtime, maintained at duty post, upon which leave input data is based.

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

WebTA operates under the following FDIC Privacy Act SORN: "30-64-0015, *Personnel Records*" (80 FR 67001).

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

No. The SORN does not require amendment or revision.

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. The system does not aggregate or consolidate data. The data is maintained at the detail level for interfaces and reporting.

The system contains security controls that protect the WebTA application from unauthorized access. Access to WebTA is granted only to those persons within the FDIC specifically authorized by the Corporation. Access levels and permission levels have been established and access provided only to those persons who have a need to know the information is contained in the system in order to carry out their duties. In accordance with Federal law, policy and regulation, WebTA has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

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 monitoring of individuals takes place with WebTA.

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 magnitude of harm would depend on the specific data, the number of records disclosed, and the use to which the improperly disclosed data is put.

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

No .