Web-based Time and Attendance (webTA) Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Web-based Time and Attendance (webTA)
Approved Date: December 12, 2016

Additional Privacy Compliance Documentation Required:

☐ None

☒ System of Records Notice (SORN)

☐ Open Data Privacy Analysis (ODPA)

☒ Privacy Act Section (e)(3) Statement or Notice (PA Notice)

☐ USAID Web Site Privacy Policy

☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents

☐ Role-Based Privacy Training Confirmation

Possible Additional Compliance Documentation Required:

☒ USAID Forms Management. ADS 505

☐ Information Collection Request (ICR). ADS 505, ADS 506, and ADS 508 Privacy Program

☒ Records Schedule Approved by the National Archives and Records Administration. ADS 502

Table of Contents

1 Introduction

The USAID Privacy Office is using this Privacy Impact Assessment (PIA) Template to gather information from program managers, system owners, and information system security officers in order to analyze USAID information technology and information collections (systems) that collect, use, maintain, or disseminate personally identifiable information (PII). See **ADS 508 Privacy Program** Section 503.3.5.2 Privacy Impact Assessments.

2 Information

2.1 Program and System Information

2.1.1 Describe the PROGRAM and its PURPOSE.

The Web Time and Attendance System (webTA) is a paperless, web-based system which provides electronic review and approval of individual time and attendance (T&A) records. WebTA is a Commercial Off-The-Shelf (COTS) product designed by Kronos Inc. exclusively for the Federal Government. The webTA application is used by USAID employees, including Direct-Hires, Personal Services Contractors (PSCs), and Foreign Service Nationals (FSNs). The webTA database is designed to capture hours worked, leave used and accounting information on a bi-weekly basis. WebTA tracks hours worked as well as current balances for the various leave buckets for each user.

For U.S. citizen employees (i.e.,U.S. Direct-Hires and U.S. PSCs), USAID transmits this T&A information to the US Department of Agriculture (USDA) National Finance Center (NFC) for payroll processing. A data refresh is performed every four weeks to re-synchronize the data in webTA with the data at NFC. For these employee types, webTA contains Social Security Numbers (SSNs). Additionally, webTA may optionally retain locator information, such as addresses and phone numbers; however, while USAID does not require these fields to be completed by its users, any individual user may opt to enter the locator information. USAID is currently researching a solution to this issue through the vendor.

For non-U.S. citizen USAID employees (i.e., Foreign Service Nationals/FSNs and Third Country Nationals/TCNs) who cannot be paid by the NFC, webTA uses an internally unique employee identifier rather than an SSN. For these employees, USAID exports T&A data from webTA (using Business Objects Enterprise) and records the information in other systems, including the Department of State Payroll Processing System, the Peachtree Accounting System, and USAID's Phoenix Financial Management System for further processing.

2.1.2 Describe the SYSTEM and its PURPOSE.

The webTA application is a COTS product developed by Kronos to track user time and attendance and to forward these payroll records to the USDA NFC at the end of each pay period.

Kronos designed webTA to improve productivity, performance, and outcomes. This system incorporates Federal-specific workforce technology architecture rules; privacy and security rules; accessibility rules; audit-ability and financial controls rules; modernization, accountability and efficiency rules; cost accounting rules; business rules; compliance rules; pay rules; work plans; work schedules; and workflows.

2.1.2 Describe the SYSTEM and its PURPOSE.

Version 4.1.28 of webTA is designed to support Single Sign On (SSO) through PingFederate as well as to provide external facing access through Netscaler. The system is backed up by separate physical servers (not virtual), currently located at the BIMC facility in Beltsville, MD. The database maintains a live link via Oracle DataGuard to continuously backup the production database in real-time. In the event of a production outage of either the web server or the database server (or both), the Disaster Recovery facility could immediately be made available with an up-to-date database to continue operations.

2.1.3 What is the SYSTEM STATUS?

☐ New System Development or Procurement

☐ Pilot Project for New System Development or Procurement

☒ Existing System Being Updated

☐ Existing Information Collection Form or Survey
OMB Control Number:

☐ New Information Collection Form or Survey

☐ Request for Dataset to be Published on an External Website

☐ Other:

2.1.4 What types of INFORMATION FORMATS are involved with the program?

☐ Physical only
☒ Electronic only
☐ Physical and electronic combined

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

☒ No.

☐ Yes:
☐ Information Collection Forms or Surveys
☐ Third Party Web Site or Application
☐ Collaboration Tool

2.1.6 What type of system and/or TECHNOLOGY is involved?

☐ Infrastructure System (Local Area Network, Wide Area Network, General Support System, etc.)

☒ Network

☒ Database

☒ Software

☒ Hardware (Dedicated USAID webTA Servers)

☐ Mobile Application or Platform

☐ Mobile Device Hardware (cameras, microphones, etc.)

☐ Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)

☒ Wireless Network

☐ Social Media

☒ Web Site or Application Used for Collaboration with the Public

☐ Advertising Platform

☒ Website or Webserver

☒ Web Application

☒ Third-Party Website or Application

☐ Geotagging (locational data embedded in photos and videos)

☐ Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)

☐ Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)

☐ Facial Recognition

☐ Identity Authentication and Management

☐ Smart Grid

☐ Biometric Devices

☐ Bring Your Own Device (BYOD)

☐ Remote, Shared Data Storage and Processing (cloud computing services)

☐ Other:

☐ None

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
☐ Citizens of the United States
☐ Aliens lawfully admitted to the United States for permanent residence
☒ USAID employees and personal services contractors
☒ Employees of USAID contractors and/or services providers
☐ Aliens
☐ Business Owners or Executives
☐ Others:
☐ None

2.2 Information Collection, Use, Maintenance, and Dissemination

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ Name, Former Name, or Alias
☐ Mother's Maiden Name
☒ Social Security Number or Truncated SSN (only collected for US Direct-Hires and USPSCs; not collected for FSNs or TCNs)
☐ Date of Birth
☐ Place of Birth
☒ Home Address – system can save this information but is not currently tracked by webTA
☒ Home Phone Number – system can save this information but is not currently tracked by webTA
☒ Personal Cell Phone Number – system can save this information but is not currently tracked by webTA
☐ Personal E-Mail Address
☒ Work Phone Number – system can save this information but is not currently tracked by webTA
☒ Work E-Mail Address – system can save this information but is not currently tracked by webTA
☐ Driver's License Number
☐ Passport Number or Green Card Number
☒ Employee Number or Other Employee Identifier
☐ Tax Identification Number

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☐ Credit Card Number or Other Financial Account Number
☐ Patient Identification Number
☐ Employment or Salary Record
☐ Medical Record
☐ Criminal Record
☐ Military Record
☐ Financial Record
☐ Education Record
☐ Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
☐ Sex or Gender
☐ Age
☐ Other Physical Characteristic (eye color, hair color, height, tattoo)
☐ Sexual Orientation
☐ Marital status or Family Information
☐ Race or Ethnicity
☐ Religion
☐ Citizenship
☐ Other:
☐ No PII is collected, used, maintained, or disseminated

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☒ Log Data (IP address, time, date, referrer site, browser type)
☐ Tracking Data (single- or multi-session cookies, beacons)
☐ Form Data
☒ User Names
☐ Passwords

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?

☐ Unique Device Identifier

☐ Location or GPS Data

☐ Camera Controls (photo, video, videoconference)

☐ Microphone Controls

☐ Other Hardware or Software Controls

☐ Photo Data

☐ Audio or Sound Data

☐ Other Device Sensor Controls or Data

☐ On/Off Status and Controls

☐ Cell Tower Records (logs, user location, time, date)

☐ Data Collected by Apps (itemize)

☐ Contact List and Directories

☐ Biometric Data or Related Data

☐ SD Card or Other Stored Data

☐ Network Status

☐ Network Communications Data

☐ Device Settings or Preferences (security, sharing, status)

☐ Other:

☐ None

2.2.4 Who owns and/or controls the system involved?

☒ USAID Office: M/CFO

☐ Another Federal Agency:

☐ Contractor:

☐ Cloud Computing Services Provider:

☐ Third-Party Website or Application Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

2.2.4 Who owns and/or controls the system involved?

☐ Other:

3 Privacy Risks and Controls

3.1 Authority and Purpose (AP)

3.1.1 What are the statutes or other LEGAL AUTHORITIES that permit you to collect, use, maintain, or disseminate personal information?

The Tax Act of 1974 authorized the collection of SSNs for processing payroll by amending Section 6109 of the IRS Code to provide that SSNs be used as the tax identification number (TIN) for all tax purposes. Additional authorities include Title 5, U.S.C. §§ 1302, 2951,4118, 4308; Sections 112 (a) and 113 of the Budget and Accounting Procedures Act of 1950; Foreign Assistance Act of 1961 (as amended) 621(a), 625, 636(b) and (c); Executive Order 10927; P.L. 93-647; Foreign Service Act of 1946, as amended; and Social Security Act (42 U.S.C. § 659).

The USAID Network (AIDNET) and USDA/NFC's Office of the Chief Financial Officer (OCFO) has an MOU/ISA in place from September 2012, and the Agency is now in the process of reviewing the MOU/ISA for potential updates.

3.1.2 Why is the PII collected and how do you use it?

The Pll collected is used to process payroll and to ensure the proper contributions to the Social Security system. It is also used to reconcile records at the NFC, which completes the payroll function. USAID made an early decision to require Timekeepers to manage user profiles, which include SSN management. Under this premise, the user and the assigned Timekeeper can view the SSN when the user's profile is retrieved. If the user determines that the SSN is not correct, the Timekeeper must correct it. Otherwise, the Timekeeper does not need the SSN for any Timekeeper functions.

3.1.3 How will you identify and evaluate any possible new uses of the PII?

The Pll information in webTA exists solely to complete payroll functions. It has no other authorized use. Only the System Owner can evaluate new system uses.

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

☐ No:

☒ Yes:

☐ Form or Survey (Please attach)

☐ OMB Number, if applicable:

☒ Privacy Act Statement (Please provide link or attach PA Statement)

3.2.3 Who owns and/or controls the personal information?

☒ USAID Office: M/CFO

☐ Another Federal Agency:

☐ Contractor:

☐ Cloud Computing Services Provider:

☐ Third-Party Web Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

3.2.8 Do you collect PII for an exclusively statistical purpose? If you do, how do you ensure that the PII is not disclosed or used inappropriately?

☐ No.

☐ Yes:

3.3 Data Quality and Integrity (DI)

3.3.1 How do you ensure that you collect PII to the greatest extent possible directly from the subject individual?

All Pll is collected directly from the individual at the time of employment. The System Owner is developing a new policy/SOP for onboarding new employees, including guidance on minimizing the collection of Pll for new employees.

3.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?

The SSN stored by the system is viewable only by the HR Administrator and Administrator. All other roles can only see the last four digits. It is made available to individuals with the HR Admin and admin roles to ensure accuracy. In addition, individual users have the ability to update their own locator information, but USAID is currently exploring options through the vendor to mask the locator field or prohibit data entry by users.

3.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?

Only the individual user and his or her Timekeeper may view or change the SSN. A recent change eliminated the Supervisor role from having the ability to view the SSNs of their subordinates. Timekeepers can only see individual records for users assigned directly to them and can only view the last four digits of the SSN for the individual assigned to a particular Timekeeper. All other records are not retrievable.

USAID performs additional validation at the time the T&A record is processed by the NFC. If the SSN does not match an existing SSN within the NFC personnel database, webTA will reject the T&A record. These transactions are captured in a payroll processing exceptions report.

3.4 Data Minimization and Retention (DM)

3.4.1 What is the minimum PII relevant and necessary to accomplish the legal purpose of the program?

The SSN is required to complete payroll functions and make relevant contributions to the Social Security Administration (SSA).

3.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

☒ No.

☐ Yes:

3.4.4 What types of reports about individuals can you produce from the system?

WebTA retrieves data twice monthly from NFC via a secure FTP, which is designated at one specific terminal and imported into the USAID WebTA database. Reports may be produced anywhere from the AidNet network and printed on AidNet network printers.

Externally, there are two methods for using webTA. The first is by logging into AidNet remotely via a system known as Server-Based Computing (SBC). This access requires a user name, a Personal Identification Number (PIN), a time-sensitive Remote SecurID Authentication (RSA) token value and a password. Attempts to print from SBC will only send documents to AidNet printers located within USAID. Printing to external printers is prohibited.

The second access method is to access the webTA URL directly (https://webta.usaid.gov). Login requirements are the same as SBC except that no password is required. Once connected, however, users may save and print to printers and storage devices local to the external location.

Email may be sent from any of the access methods above, including directly from AidNet computers. Additionally, Internal USAID systems monitor instances of SSNs that are emailed to external locations, but these systems are far from fool-proof.

3.4.6 Does the system monitor or track individuals?

(If you choose Yes*, please explain the monitoring capability.)*

☒ No.

☐ Yes:

3.5 Individual Participation and Redress (IP)

3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?

The individual consents to the use of his/her SSN as a condition of employment. In addition, the individual enters webTA at the Splash page must accept the terms and conditions, which includes a Privacy Act Statement or Notice, prior to entering their T&A information.

3.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

The SSN is accessible to the user through a personal profile record. The user cannot edit the record but can ask the Timekeeper or a System Administrator to update the record if it is incorrect. In addition, currently, the webTA System may optionally retain locator information such as addresses and phone numbers. While USAID does not require these fields to be completed by its users, any individual user may opt to enter the locator information.

USAID is currently researching a solution to this issue through the vendor.

3.5.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that the PII will be available to individuals who request access to and amendment of their PII?

N/A

3.7 Transparency (TR)

3.7.1 Do you retrieve information by personal identifiers, such as name or number?

(If you choose Yes*, please provide the types of personal identifiers that are used.)*

☐ No.

☒ Yes: Timekeepers, supervisors and other elevated roles can search for users by name. Employees with Admin and HR Admin roles may search by SSN as well. These searches can be filtered by status (active, inactive), organization, employee type and pay period. Timekeepers, however, will only be allowed to view the partial SSN for the employees under their purview, supervisors and their subordinates will no longer be able to view any portion of the SSN.

3.7.2 How do you provide notice to individuals regarding?

1) The authority to collect PII:

2) The principal purposes for which the PII will be used:

3) The routine uses of the PII:

4) The effects on the individual, if any, of not providing all or any part of the PII:

Notice is provided to users at the Splash or Banner Page of webTA prior to entering their data. Notice will also be provided via the onboarding documentation.

3.7.3 Is there a Privacy Act System of Records Notice (SORN) that covers this system?

☐ No

☒ Yes: USAID-16 Employee Time, Attendance, and Payroll System of Records, 80 FR 481 (January 6, 2015)

3.7.4 If your system involves cloud computing services, how do you ensure that you know the location of the PII and that the SORN System Location(s) section provides appropriate notice of the PII location?

N/A

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

The webTA web site can only be accessed by users who have been granted access by webTA System, Administrators or Human Resource Administrators. The system utilizes role-based access, which is determined by individual's job responsibilities: employee, payroll officers, Timekeepers, and System and Database Administrators.

Individuals have access only to their data. Timekeepers have access to data for their assigned Office/Bureaus employees. Some contractors have administrative access necessary to maintain the web site. Additionally, some non-paid users are provided access to the webTA system in order to act as Timekeepers. This Timekeeper role provides them with access only to user records assigned specifically to them.

3.8.3 With whom do you share the PII outside of USAID? And whether (and how, if applicable) you will be using the system or related web site or application to engage with the public?

The webTA application shares the Pll for with the USDA NFC, which is responsible for completing the payroll process for USAID employees. There is no engagement with the public. USAID connects with NFC through a specified list of IP addresses to download flat files from NFC to upload into webTA.

3.8.4 Do you share PII outside of USAID? If so, how do you ensure the protection of the PII 1) as it moves from USAID to the outside entity and 2) when it is used, maintained, or disseminated by the outside entity?

☐No.

☒ Yes: This system only shares Pll with the USDA NFC, which completes the payroll function for USAID employees. USDA/NFC issues credentials to the USAID personnel who initiate the transfers, and the NFC renews these credentials annually. The FTP file transfer from USAID directly to the NFC is encapsulated by a secure, encrypted, end-to-end VPN tunnel. USAID has had an MOU/ISA in place since September 2012. The Agency is in the process of reviewing the MOU/ISA for potential updates.

3.9 Third-Party Web Sites and Applications

3.9.1 What PII *could be made available* (even though not requested) to USAID or its contractors and service providers when engaging with the public?

The webTA web site can only be accessed via a web browser. While the webTA web site can be accessed by any device capable of accessing the Internet, no provision is made for small screens rendering small mobile devices useless in rendering the time sheet which is the main action for most webTA users.

Pll available in the system is stored encrypted in the database and is not shown to users other than the user and his or her assigned Timekeeper. This information is only shared with NFC for the purpose of completing the payroll process. While Timekeepers may view the last four digits of the employees under their purview, the full SSN will be masked for all other users, including supervisors.

Appendix A. Links and Artifacts

A.1 Privacy Compliance Documents or Links

☐ None. There are no documents or links that I need to provide.

☐ Privacy Threshold Analysis (PTA)

☐ Privacy Impact Assessment (PIA)

☐ System of Records Notice (SORN)

☐ Open Data Privacy Analysis for Posting Datasets to the Public (ODPA)

☒ Data Collection Forms or Surveys

☐ Privacy Act Section (e)(3) Statements or Notices

☐ USAID Web Site Privacy Policy

☐ Privacy Policy of Third-Party Web Site or Application

☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents