Phoenix Financial System Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Phoenix Financial System
Approved Date: May 16, 2017

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 United States Agency for International Development (USAID) is the lead U.S. Government agency that works to end extreme global poverty and enable resilient, democratic societies to realize their potential. The USAID mission states: The Agency partners with others to end extreme poverty and promote resilient, democratic societies while advancing our security and prosperity.

The Financial Systems Division (M/CFO/FS) supports USAID's financial management operations and the Agency's ability to effectively and efficiently analyze, allocate, and report on foreign assistance funds. M/CFO/FS helps the Agency achieve its performance measurements, which include timely financial reporting, elimination of material weaknesses in internal control, the achievement of unmodified ("clean") audit opinions, and implementing financial management systems and processes that meet Federal requirements. Further, M/CFO/FS manages the development and implementation of Phoenix, USAID's worldwide financial system. M/CFO/FS provides operational support and security administration for Phoenix, and coordinates with M/CIO staff, Department of State, Office of Inspector General (OIG), contractors, system owners, and other stakeholders as necessary to maintain the financial system.

2.1.2   Describe the SYSTEM and its PURPOSE.

Phoenix is the USAID financial system and the Agency's accounting system of record based on a COTS package and configured for USAID operations. Phoenix includes modules such as General Ledger, Accounts Payable, Accounts Receivable, and Budget Execution, which are required to perform necessary accounting operations. Phoenix must conform to strict regulatory audit requirements promulgated by the Office of Management and Budget, the Department of Treasury, and the General Accountability Office.

Phoenix is a USAID system and major application hosted at the Department of State's Global Financial Management Center in Charleston, SC. It has been hosted at Department of State since 2006 at the direction of OMB and the Office of the Inspector General at both Dept. of State and USAID. Users of Phoenix and its data are located in the Washington, DC metro area (headquarters) and in about 50 missions worldwide. It is accessible *only* from internal USAID and Department of State networks (AIDNET and Opennet). On these secure networks, Phoenix is accessible via Username and Password and via Single Sign-On enabled by the Agency's chosen federated identity management solution, PingIdentity's PingFederate. There is not a mobile app or mobile-enabled method of accessing Phoenix.

Using secure File Transfer Protocol (FTPS), Phoenix securely imports detailed payroll data into its ePayroll module from USDA's NFC for summarizing into accounting records, before exporting the detailed data to the USAID Payroll Reporting Database for historical records also through the use of FTPS.

2.1.2 Describe the SYSTEM and its PURPOSE.

Using FTPS, Phoenix securely imports travel information from the USAID E2 Travel system for purposes of verifying travel authorization and funding, and to reconcile travel accounting information with actual trips.

Phoenix has interfaces with various other internal and external systems, but the two above are the only interfaces involving the transfer of what might be considered PII under the Privacy Act and Treasury Financial Manual Chapters 9200, A123, A130, and A136.

The following interfaces are either inbound or outbound:

Citibank (Credit Card) Interface
DHHS Inbound Interface (non-pooled)
DHHS Inbound Expenditure Interface (pooled)
DHHS Inbound Advance Interface (pooled)
DHHS Outbound Interface
E2 Interface
Midlands/PNC Interface
NFC Interface
USPSC Transfer Interface
USDO Interface
Treasury Automated Disbursement Interface
IRS 1099 Interface
U.S. Department of State Disbursement Interface

The following are excerpts from *Phoenix 7.2.1 Technical Architecture, version 6.0, dated May 26, 2016.* regarding the system's reporting database, REPT:

4.1 Physical Data Architecture:

The Phoenix Suite applications rely on a RDBMS as its underlying data storage mechanism. As described in Section 3.5, the database server hardware consists of one HP Proliant BL460c blade server running on the Windows Server 2012R2 64-bit platform. The databases run on Oracle 12c Release – 12.1.0.2 64bit Enterprise Edition. While the Phoenix OLTP database is hosted at CGFS, the reporting database (REPT) is hosted on a database server located at the TCOC in TerreMark's facility in Miami, FL. To populate the reporting database with up-to-date data, a nightly replication process moves all changed data to staging databases at TCOC using NetApp SnapMirror.
• Every three hours SnapMirror syncs the PPX1 volume at CGFS which contains the Phoenix production database with the PHXHOLD volume, located at the TCOC, and the PPX1 volume located at the DR site located at BIMC in Beltsville, MD.
• After the PHXHOLD volume has synced with the volume at CGFS, a SnapMirror process syncs PHXHOLD to another holding volume located at TCOC (labeled Drive I, in Exhibit 4-1).
• NetApp Snapshot is then used to copy this new volume and refresh the replicated production database (PPX2), the Phoenix debug database (QPX1), and the PPX1 prime (PRIM) database.
• PPX2 is then used as the source database for the extract, transform, and load (ETL) process which populates REPT with new data. Section 5 describes the ETL process in further detail.
• Immediately after PRIM has been refreshed, it is booted in restricted mode and sensitive data is scrubbed from the database. PRIM is then used as the source database for any refreshes to the development and test environments.

4.3 Databases:

Phoenix makes use of two databases: the Phoenix OLTP database named PPX1, which contains all transactional

2.1.2 Describe the SYSTEM and its PURPOSE.

data generated by the system; and the Phoenix Reporting database named REPT, which is a subset of custom reporting tables and denormalized data from the OLTP database to provide more efficient reporting capabilities. Phoenix reporting and the Phoenix reporting database is discussed in Section 5. The Phoenix OLTP database is broken up into several different schemas based on recommended configuration for Momentum. Each schema is broken out by its role within the application suite.

5.1 Reporting Databases:

This section, along with Exhibit 5-1, provides an overview of the Reporting Databases (i.e., PPX2, PPY1 and REPT) and the nightly refresh.

The Reporting Databases provide a separate source of data which is designed to minimize the performance impact of reporting against Phoenix Production and maximize performance in generating reports. The Reporting Databases consists of three database instances: PPX2, which is a snapshot of PPX1; PPY1, which is used as the primary data store for historical payroll data, and REPT, which contains custom reporting tables that are synchronized with PPX2 and PPX1. Data in the Reporting Phoenix 7.2.1 Technical Architecture Phoenix 7.2.1 – Technical Architecture Reporting and Other Tools Revised: May 26, 2016/Final Version 6.0 5-31 Databases is one day old. PPX2 is available to reporting tools that require Phoenix data which is not readily available in REPT.

REPT and PPY1 are updated through nightly ETLs (Extract, Transform and Load) of PPX2 data, which begins at 7pm EST and can last several hours. During this period the Reporting Databases and the reporting tools that rely on it are not available to users.

Data in REPT is denormalized during the ETL process to improve performance and facilitate report generation. The ETL process uses a series of Oracle database procedures written in SQL and PL/SQL, which are initiated through BMC software's Control-M workload automation software. The ETL process updates REPT with new Phoenix transactions that have occurred since the previous update. Data in REPT is stored in tables at various levels of detail, including transaction detail, multi-dimensional summaries, reference data and metadata.

Custom BIRT reports, BOE, PhoenixViewer, and PhoenixViewer Exec-Info use the Reporting Databases. The GLAAS operational data source, ODS, also accesses a subset of Phoenix tables that are extracted in a separate process.

Data is also exchanged between the system and GLAAS and E2. MOUs between Phoenix Financial System and those systems are attached.

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: The user functionality and formatting of the system is being updated.

Specifically, the arrangement of the screens used for entering data will be changed. In addition, the data at rest in Phoenix is undergoing the process to be encrypted. The target completion date for this process is March 2017.

☐ 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

☐ Mobile Application or Platform

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

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

☐ Wireless Network

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

☐ 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: USAID vendors (in cases where they are individuals). Any of the marked categories could be a "vendor."

☐ 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
☐ Date of Birth
☐ Place of Birth
☐ Home Address
☐ Home Phone Number
☐ Personal Cell Phone Number
☐ Personal E-Mail Address
☒ Work Phone Number
☒ Work E-Mail Address
☐ Driver's License Number
☐ Passport Number or Green Card Number
☐ Employee Number or Other Employee Identifier
☒ Tax Identification Number
☒ Credit Card Number or Other Financial Account Number (bank 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

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☐ Other Physical Characteristic (eye color, hair color, height, tattoo)
☐ Sexual Orientation
☐ Marital status or Family Information
☐ Race or Ethnicity
☐ Religion
☐ Citizenship
☒ Other: Bank account information to authorize an ACH transaction through Treasury or USDO; Travel information, including traveler name, month/year of travel, and destination, is needed for to issue travel authorizations and validate funding availability; home addresses are not entered into Phoenix, but an address is entered into Phoenix from IRS Form 1099, for example.
☐ 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
☐ 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)

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ 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:
☐ 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?
Phoenix maintains and disseminates only PII related to payroll processing as required by law for IRS purposes. SSN are only sent to IRS as part of 1099 processing.

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

The information is collected for payroll and accounting purposes only. Phoenix is a financial system and USAID's accounting system of record. Phoenix maintains summary or detailed transactions resulting from budgetary and proprietary financial activity. The system does not process direct deposit transactions. The PII is collected to provide notice to payor departments and agencies, like Treasury, that a transaction should be executed.

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

All changes to the Phoenix data are reviewed for PII. In cases where PII is identified, controls are designed and implemented to limit access to and dissemination of the PII. Since the data collected is only that of employees or vendors, consent is implicit in doing business with or being employed by USAID.

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?

Phoenix receives PII from feeder systems and performs no collection itself; thus, it relies on the feeder systems to ensure that PII comes directly from the data subject where possible. For example, travel related data is imported from E2 Travel and changes, if needed, are entered through that system. That information is entered by the user/owner of the PII.

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?

PII is all imported from NFC and E2 Travel. Phoenix receives PII from feeder systems and performs no collection itself. Feeder systems are relied on to ensure the PII is accurate, timely, relevant, and complete at the time of collection. The integrity of the import processes is monitored for accuracy.

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

Data is input only from the feeder systems. Any corrections originate from those systems. The following interfaces are either inbound or outbound:

Citibank (Credit Card) Interface
DHHS Inbound Interface (non-pooled)
DHHS Inbound Expenditure Interface (pooled)
DHHS Inbound Advance Interface (pooled)
DHHS Outbound Interface
E2 Interface
Midlands/PNC Interface
NFC Interface
USPSC Transfer Interface (Limited payroll transactions containing transaction-level payroll information for United States Personal Service Contractors (USPSC) are extracted from the data downloaded from the NFC Interface process above. PSCs are reported on differently than DH.)
USDO Interface
Treasury Automated Disbursement Interface
IRS 1099 Interface
U.S. Department of State Disbursement Interface

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?

SSNs are needed for reporting payroll to the IRS on 1099s. They are mandated by law for this use.

Travel information, including traveler name, month/year of travel, and destination, is needed for to issue travel authorizations and validate funding availability.

Bank account information is required to provide appropriate transaction instructions to payor departments or agencies.

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?

There is a small set of payroll-related reports produced that contain SSNs. Those are printed with privacy warnings and access to these reports is limited to only those roles which require them, including Document Control Clerks, Voucher Examiners, and Certifying Officers involved in the cash management and payment process. In general, payroll information passes through Phoenix and is not retained in detail. It is summarized into ledger transactions and retained as accounting entries with no PII attached.

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?

No.

PII is imported only from the feeder systems mentioned above. Consequently, Phoenix relies on the feeder systems to obtain consent to collect PII. The PII imported from the feeder systems is a requirement of working for or doing business with USAID.

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 feeder systems interface with data subjects and are accountable for enabling access and amendment of PII by the data subject. (Phoenix is only accessible by authorized Phoenix users and only.) Phoenix users with specific roles are able to access PII but are not able to amend it. Information can be accessed through a FOIA request as well.

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?

Cloud computing services are not employed by Phoenix.

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: (PII elements are not a primary key. Phoenix is an accounting system, not an HR system. Data is routinely retrieved by contract number, BBFY, fund type, etc. but not by personal identifiers. However, data can be retrieved by a person's name, such as that of a PSC, or vendor ID number. A PSC's vendor ID number is unique to that person and can appear across multiple entries in the system.)

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:

NA – PII is not collected from individuals by Phoenix. The system therefore must rely on feeder systems to provide these details.

SORN: USAID-33 has been published.

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

☐ No

☒ Yes: USAID-33

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?

Cloud computing services are not employed by Phoenix.

3.8   Use Limitation (UL)

3.8.1	Who has access to the PII at USAID?

Certifying Officers, Document Control Clerks, Voucher Examiners require access to PII in order to process payments and have specific roles in Phoenix, i.e. CERTOFCR, DOCTLCL2, DOCTLCLK, VCHREX2, VCHREXM.

USAID employees and contractors maintaining the vendor database will have read access to the vendor data which includes individuals doing business with USAID. These staff will have specific roles in Phoenix, i.e., VENDACCEPT, VENADMIN, VENCREATE, VENDREVIEW, VENDVIEW. They cannot modify the PII as it must be modified from the feeder system to maintain the integrity of the data stream.

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?

Phoenix is not a publicly-accessible system. PII is shared only with the IRS for 1099 delivery.

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: PII is sent out of Phoenix only in the form of 1099s delivered to IRS and subject to the controls IRS has implemented for that process.

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?

NA – Phoenix does not engage with the public nor is it publicly-accessible.

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