Management Bureau/Chief Information Officer/Information Assurance
(M/CIO/IA)

PRIVACY IMPACT ASSESSMENT (PIA)

ePerformance

Cornerstone OnDemand Integrated Talent Management System (ITMS)

Approved: February 25, 2014

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).

The PIA process should accomplish two goals: 1) determine the privacy risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate and enforce protections and alternative processes for handling PII to reduce potential privacy risks to acceptable levels.

Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable. Each section includes assistance (in blue text) on how to answer the question. For additional instructions on how to complete this PIA Template, please see Appendix C Conducting the PIA.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at privacy@usaid.gov.

2. INFORMATION

2.1 PROGRAM INFORMATION

2.1.1 Describe the program and its purpose.

The ePerformance project will facilitate the automation of existing HR Performance Management Policies and Procedures through the existing Performance module within the Cornerstone OnDemand Integrated Talent Management System (ITMS). The Performance module is a 100% configurable process integration piece that allows administrators to build custom workflows for Performance Management processes. In this way, USAID Performance Management processes will be fully automated, eliminating paper/Microsoft Word based performance plans and creating clear transparency/reporting for the Office of Human Resources (OHR) and USAID Rating Officials. The program operates worldwide, and impacts Senior Executive Service, Civil Service. and Foreign Service employees.

The ePerformance project leverages the existing information available in the Cornerstone OnDemand application, which facilitates USAID University. The following information is provided through an existing integration with HRConnect (HRC).

Cornerstone OnDemand can maintain the following types of data:

- User Records
- Training Histories
- Performance Scores
- Compensation Actions (bonus, merit pay increase, lump sum payout)
- Competency Assessments
- Employee Profile
- Succession Plans
- The Cornerstone OnDemand (CSOD) data elements are mapped to their corresponding HRConnect (HRC) data elements, and there are customizable data fields as well.

2.1.2 What types of paper documents, systems, electronic media, digital collaboration tools or services, and/or mobile services do you employ to collect, use, maintain, and disseminate information?

Cornerstone OnDemand receives information through an existing integration with the HR system of record, HRConnect. HRConnect is managed and maintained by the OHR Information Management team and transfers a Pretty Good Protection (PGP) encrypted file containing the most recent data for the HRConnect/Cornerstone mapped data fields to the Cornerstone OnDemand hosted SFTP. All other information that is collected, used, maintained and/or disseminated from the Cornerstone OnDemand application is manually entered by system administrators . Only users with the approved level of access from USAID and the Department of Treasury have access to information stored within the application.

2.1.3 How do you retrieve information?

Data may be reviewed through the user interface after authentication to the system. The user interface supports both screens that display the information and reports. The following classes of users will have some type of rights to view the individual's information on a limited basis:

- The employee
- The employee's manager
- The employee's AMS Officer
- The employee's EXO (If applicable)
- ePerformance Administrators

2.2 INFORMATION COLLECTION, USE, MAINTENANCE, AND DISSEMINATION

2.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other*, please list the additional types of PII.)*

☒ 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 (Unique HRConnectID; SSNs are not stored within Cornerstone OnDemand)
☐ Tax Identification Number
☐ Credit Card Number or Other Financial Account Number
☐ Patient Identification Number
☒ Employment or Salary Record

2.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate? *(Please check all that apply. If you choose* Other*, please list the additional types of PII.)*
☐ Medical Record
☐ Criminal Record
☐ Military Record
☐ Financial Record
☒ Education Record
☐ Biometric Record (signature, fingerprint, photograph, 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: Additional PII that is voluntarily provided by the complainants and others submitting pertinent information and OCRD collects documents, such as emails, related to the complainant that might contain PII.
☐ None

2.2.2 About whom do you collect personal information? *(Please check all that apply. If you choose* Other*, please provide the types of people.)*
☐ Citizens of the United States
☐ Aliens lawfully admitted to the United States for permanent residence
☐ USAID employees, including Foreign Service National (FSN) Direct Hires, FSN Personal Services Contractors, and Third Country National Employees (non-US citizens for informal EEO process only)
☐ Employees of USAID contractors or service providers (for informal EEO process only)
☐ Visitors to the United States
☐ Aliens
☐ Business Owners or Executives
☐ Others: USAID Direct Hires only, including Senior Executive Service, Foreign Service, and Civil Service.

2.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate? *(Please check all that apply. If you choose* Other*, please provide the types of data.)*
☒ 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)

2.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate? *(Please check all that apply. If you choose* Other*, please provide the types of data.)*
☐ 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 What PII, digital data, or mobile data *could be* made available to USAID or its contractors and service providers?
Provided that contractors and/or service providers have been cleared for access through USAID and approved through the Department of Treasury for elevated access, they may gain access as needed to the PII that has been outlined within the tables above. Contractors or service providers who are cleared for general use of the application will have no access to PII. Mobile services are not included in ePerformance.

2.2.5 What are the authorities that permit you to collect, use, maintain, or disseminate PII and, specifically, Social Security Numbers (SSNs)?
Social Security Numbers are not collected, used, maintained, or disseminated through the Cornerstone OnDemand application.

2.2.6 Who owns and/or controls the PII? *(Please check all that apply. Please provide the names of the specific organizations. If you choose* Other*, please provide the types of organizations and the name of each organization.)*
☒ USAID Office: OHR
☐ Another Federal Agency:
☒ Contractor:
☐ Cloud Computing Services Provider:

2.2.6 Who owns and/or controls the PII?

(Please check all that apply. Please provide the names of the specific organizations. If you choose Other, *please provide the types of organizations and the name of each organization.)*

☐ Third-Party Web Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

2.2.7 Who has access to the PII at USAID?

Access to PII in Cornerstone OnDemand is restricted depending on the security role/access level of individuals within the application. Additionally, elevated access is requested through, and granted by the shared service center support team at the US Department of Treasury through the completion of the form linked below:

2.2.8 With whom do you share the PII outside of USAID?

Currently there are two organizations outside of USAID who have access to PII through the Cornerstone OnDemand application. The users below all have direct access to USAID's Cornerstone OnDemand environments for technical and project support purposes.

Department of Treasury – Shared Service Center
Cornerstone OnDemand

2.3 SYSTEM INFORMATION

2.3.1 Describe the system and its purpose.

Cornerstone OnDemand is a comprehensive talent management system that incorporates the following functional modules:

- Learning
- Connect
- Performance
- Succession
- Compensation Management
- Extended Enterprise

The Learning module supports the management and tracking of training events and individual training records. Training events may be instructor led or online. Courses may be managed within the system to provide descriptions, availability, and registration. Online content is stored on the system. Training information stored for individuals includes courses completed, scores, evaluation scores and courses that employee is registered to attend/complete.

The Connect module supports employee collaboration efforts. Features include communities of practice , expertise location, biogs, and knowledge sharing support. Profile information that may be stored by the system includes job

2.3.1 Describe the system and its purpose.

position, subject matter expertise, and previous accomplishments.

The Performance module (ePerformance) supports management of organizational goals and alignment of those goals to individual performance. The module supports managing skills and competencies for the organization. The module also supports employee performance reviews. The types of information gathered about employees include their skills, competencies, and performance evaluation.

The Succession module supports workforce management and planning. The type of information gathered for this module includes prior work experience, skills, and competencies.

The Compensation Management module supports compensation and awards planning. The type of information gathered for this module includes base salary pay plan, pay plan step, locality pay adjustments, market adjustments, lump sum payments, prior bonus and award amounts employee received and performance evaluation final score.

The Extended Enterprise module supports delivery of training outside of the organization . Training provided may be for a fee. The type of information collected for this module includes individual data for identifying the person for training records management and related information for commercial transactions.

2.3.2 What type of system and/or technology is involved?

(Please check all that apply. If you choose New Technology *or* Other, *please explain.)*

☐ 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
☐ Social Media
☐ Advertising Platform
☐ Website or Webserver
☒ Web Application (Treasury Share Service)
☒ Third-Party Website or Application (Cornerstone OnDemand)
☐ Geotagging (locational data embedded in photos and videos)
☐ Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)

2.3.2 What type of system and/or technology is involved? *(Please check all that apply. If you choose* New Technology *or* Other*, please explain.)*
☐ 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: Single Sign On
☐ None

2.3.3 What is the system status? *(If this is an existing Information Collection, please enter the OMB Control Number. If you choose* Other*, please explain.)*
☐ New System Development or Procurement
☐ Existing System Being Updated
☐ Existing Information Collection OMB Control Number:
☐ New Data Collection Form or Survey
☒ Other: Existing System and Functionality Being Configured and Made Available.

2.3.4 Do you use new technology or technology used in ways not previously used by USAID? *(If you choose* Yes*, please provide the specifics of any new privacy risks and mitigation strategies.)*
☒ No.
☐ Yes:

2.3.5 Who owns and/or controls the system involved? *(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)*
☒ USAID Office: OHR – Client/Owner
☒ Another Federal Agency: Department of the Treasury – Shared Service Provider
☐ Contractor:
☒ Cloud Computing Services Provider: Cornerstone OnDemand – Cloud Application Service Provider for the Department of the Treasury.
☐ Third-Party Website or Application Services Provider:
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:

2.3.6 Who is involved in the development and/or continuing operation of the system and/or technology? *(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)*
☐ Mobile device manufacturer or other equipment manufacturer:
☒ Application Developer: Cornerstone OnDemand
☐ Content Developer or Publisher:
☐ Wireless Carrier:
☐ Advertiser:
☐ Equipment or Device Vendor:
☐ Device User:
☐ Internet Service Provider:
☐ Third-Party Data Source (Data Broker):
☐ Other:

3. PRIVACY RISKS AND CONTROLS

3.1 AUTHORITY AND PURPOSE (AP)

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

The PII that is collected through the existing integration with HRConnect, and is used to identify and populate user specific attributes within the ePerformance module.

3.1.2 What are your processes and procedures for identifying and evaluating any proposed new uses of the PII?

Any requests for new uses of the PII is requested through the Department of the Treasury Shared Service Center for identifying and evaluating proposed uses of PII.

3.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

3.2.1 Do you use any data collection forms or surveys?

(If you choose Yes*, please provide the OMB Control Number and USAID control number.)*

☐ No.

☒ Yes. The Department of the Treasury is using their accountability, audit, and risk management policies and procedures to safeguard PII.

3.2.2 If the PII is being migrated from a legacy system to a new system, what safeguards are in place to mitigate the privacy risks of transferring the PII from the old to the new system?

Not Applicable. No data migration is involved.

3.2.3 What privacy requirements have you included in contracts and other acquisition-related documents, pursuant to the Federal Acquisition Regulation (FAR) and compliance with the Privacy Act, FISMA, and other privacy requirements?

ePerformance is in accordance with FEDRAMP mandates through the Department of C&A process.

3.2.4 What requirements have you included in contracts and other acquisition-related documents to ensure that 1) USAID owns and controls the PII in the system for the length of the contract and beyond, 2) the contractor or service provider has no ownership of the PII, and 3) the contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract during the life of the contract?

The Blanket Purchase Agreement (BPA) between the Department of the Treasury and Cornerstone OnDemand (CSOD) provides for Government ownership of all data, to include that which is personally identifiable. Furthermore, it specifies that CSOD shall provide all data to the Department of the Treasury at the end of the contract, upon request, in a manner that preserves all relationships and integrity. Th.is approach would then allow Department of the Treasury to return the data to USAID. Our BPA with CSOD stipulates that government data is provided on a For Official Use Only (FOUO) basis and is to be destroyed according to the DOD method when no longer needed (i.e. conclusion of the contract).

3.2.5 How do you audit and/or monitor system and user activity to ensure that the administrative, technical, and physical security safeguards you use actually do guard against privacy risks?

Audit logs are protected from unauthorized access and modifications via the use of firewalls, intrusion detection devices, access polices, etc. This is described and covered by the Department of Treasury's System Security Plan.

3.2.6 How do you ensure that USAID employees, contractors, and service providers understand their responsibility to protect PII and the procedures for protecting PII?

USAID enforces mandatory security and cyber awareness training annually for all USAID employees, contractors and service providers. In addition, prior to being granted elevated access to the Cornerstone OnDemand application, all users must complete and sign the Administrator Access Form referenced above.

3.2.7 If you collect PII under a pledge of confidentiality for exclusively statistical purposes, how do you ensure that the PII is not disclosed or used inappropriately?

Not Applicable.

3.2.8 What other risks to privacy exist and how do you manage these risks?

To protect PII and identify and manage risks the following controls and tools are leveraged:

- Audit logs are protected from unauthorized access and modifications via the use of firewalls
- Intrusion Detection Devices
- Enforcement of Access Policies and Procedures

These and other controls are described and covered by the Department of the Treasury's System Security Plan, which is available for review, in person, at the Department of Treasury.

3.3 DATA QUALITY AND INTEGRITY (DI)

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

PII in Cornerstone OnDemand is collected from HRConnect. The explanation for this is relatively straight forward: Cornerstone OnDemand was implemented in tandem with HRConnect as an HR Line of Business revamp and is integrated with the system of record to create and manage user accounts. Minimal PII is received from HRConnect to manage this process.

Mobile data access is not leveraged.

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 within Cornerstone OnDemand is maintained through an existing integration with the HR system of record, HRConnect, to ensure that PII is accurate, relevant, timely, and complete at the time of collection. Data collection/updates occur nightly to maintain data integrity between the two databases.

The data is verified through the approval process, which includes employees, managers and administrators, as well as user acceptance testing during implementation, which ensures the automated processed function as designed.

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

The HR system of record, HR Connect will automatically reconcile any inaccurate or outdated PII in Cornerstone OnDemand. In addition, regular audits of user records are performed to ensure that PII within the system is correctly updated and maintained. Any outliers are sent to the HR HelpDesk for correction.

3.4 DATA MINIMIZATION AND RETENTION (DM)

3.4.1 What are the minimum PII elements that are relevant and necessary to accomplish the legal purpose of the program?

(If you choose Yes*, please explain the business need for the PII elements.)*

The minimum PII element that are relevant and necessary to accomplish the legal purpose of this system include:

- Employer First Name & Last Name – included in audit trails, reports, transcripts, and performance actions
- Employee ID (USERID & UserName – Unique identifier for facilitating HRConnect Integration
- Work Email Address – Unique identifier used to authenticate Single Sign On (SSO) and facilitates notification delivery to users from the application.

The purpose of the PII collected is for the maintenance and support the employee's official personnel folder (OPF) or other agency-designated office.

3.4.2 How do you monitor the PII and the system to ensure that only the PII identified in the privacy notices is collected, used, maintained, and disseminated by the system and that the PII continues to be necessary to accomplish the legally authorized purpose?

Only the PII received through HRConnect integration is collected.

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?

(If you choose Yes*, please explain.)*

☒ No.

☐ Yes:

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

The following types of reports are available in the system:

Human resource data
Performance management

The reports are used for the following purposes:

Verification of data accuracy
Performance management – identifying learning and development needs, finding organizational strengths, tracking organizational goals

The following classes of users will have some type of rights to view reports:

The employee – for the employee only
The employee's supervisor – for the supervisor and their subordinates
The employee's AMS Officer – for supervisors and employees within the Bureaus and Offices for which they are responsible.
The employee's EXO (If Applicable) – for supervisors and employees within the Mission(s) for which they are responsible.
ePerformance Administrators – for employees for whom they have been granted view permissions for a segment of the population

3.4.5 How do you file, maintain, and store the PII? How long do you retain the PII? What methods do you use to archive and/or dispose of the PII? How do you ensure that the records management retention rules specified above are followed?

The system complies with Department of the Treasury Directive 80-50 Records and Information Management Manual. In accordance with TD 80-50, records are not destroyed or otherwise alienated from the system except in accordance with procedures prescribed in 36 CFR, Part 1228.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes: Cornerstone OnDemand tracks and maintains an audit log and on action log of all user actions made within the application.

3.4.7 What policies, procedures, and control methods do you follow to minimize the use of PII for and protect PII during testing, training, and research?

Cornerstone OnDemand is a 100% configurable, Software as Service (SaS), cloud-based solution provided through the Department of the Treasury Shared Service Center. PII is not used in the process of testing, training, or research.

3.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

3.5.1 What opportunities for consent do you provide to individuals regarding what PII is collected and how that PII is shared?

Not applicable. PII is not collected directly from the individual. It is extracted from HRConnect.

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?

Individuals are able to access and amend their own PII through HRConnect. Access to update PII in Cornerstone OnDemand is not provided, and any changes made to information within Cornerstone OnDemand, would be overwritten/corrected by HRConnect within one business day.

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 and redress?

All changes to PII must be requested and updated through HRConnect. Any changes will be reflected in Cornerstone OnDemand after one business day.

3.6 SECURITY (SE)

3.6.1 How do you secure the PII? What administrative, technical, and physical security safeguards do you use to guard against privacy risks such as 1) data loss or breach; 2) unauthorized access, use, destruction, or modification; 3) unintended or inappropriate disclosure; or 4) receipt by an unauthorized recipient?

Access within Cornerstone OnDemand is limited to the individual, their manager, and users approved for elevated access. The following security safeguards are employed to guard against privacy risks:

- Audit logs are protected from unauthorized access and modifications via the use of firewalls
- Intrusion Detection Devices
- Enforcement of Access Policies and Procedures

These and other controls are described and covered by the Department of the Treasury's System Security Plan.

3.6.2 If your system is controlled by a contractor or service provider, what requirements have you included in contracts and other acquisition-related documents to detail the procedures for privacy breach liability and response?

The Department of the Treasury BPA requires CSOD to follow applicable security procedures. These procedures are outlined within the System Security Plan as well as Interconnection Security Agreements and Memoranda of Understanding between CSOD and the Department of the Treasury. Liability in the event of a breach is not directly addressed in our documentation or agreements.

3.7 TRANSPARENCY (TR)

3.7.1 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; and 4) the effects on the individual, if any, of not providing all or any part of the PII?

All PII is collected and disseminated through HRConnect. The following notice is made available through the welcome page of the Cornerstone On Demand application:

This is a Federal Government computer system. The Federal Government computer systems are provided for the processing of Official U.S. Government Information Only. All data contained on the Federal Government computer systems is owned by the Federal Government and may, for the purpose of protecting the rights and property of the Federal Government, be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.

THERE IS N O RIGHT OF PRIVACY IN THIS SYSTEM.

System personnel may give to law enforcement officials any potential evidence of crime found on Federal Government computer systems.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISCLOSURE.

WARNING WARNING**WARNING**

3.7.2 Have you or will you publish a Privacy Act System of Records Notice (SORN) for this system? *(If you choose* Yes*, please provide information about the SORN, including the name, date, and Federal Register citation.)*
☐ No
☒ Yes: A SORN is in effect for this system. It is Office of Personnel Management OPM/GOVT-1

3.7.3 If your system involves cloud computing services and the PII is located outside of USAID, 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?
The Department of the Treasury believes that the PII aspects of this question are covered by the Privacy Impact Assessment (PIA). The System Security Plan details the control of access to PII by CSOD personnel. The BPA with CSOD stipulates that government data is provided on an For Official Use Only (FOUO) basis and is to be destroyed according to the DOD method when no longer needed (i.e. conclusion of the contract).

3.8 USE LIMITATION (UL)

3.8.1 How do you monitor access to and use of the system to ensure that the PII is collected, accessed, and used only 1) for the authorized purposes and 2) by authorized USAID employees, contractors, and service providers?
Access to the Cornerstone OnDemand is enforced through three separate mechanisms: 1. Treasury monitors access and requires compliance to proper access requests to the application. 2. Accounts and access will be added removed based on the nightly data feed from HRConnect to Cornerstone OnDemand 3. USAID email addresses are used to authenticate Single Sign On, as such once accounts are deactivated in active directory users will no longer be able to access the system.

3.8.2 If you share PII outside of USAID, 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?

(If you choose Yes, please provide the specifics of the agreement or a copy of the agreement.)

Not applicable. PII is not moved outside of USAID to other entities.

3.9 THIRD-PARTY WEBSITES AND APPLICATIONS

3.9.1 What PII might become available to you when the third-party website or application makes information available to you through public use?

Not Applicable

3.9.2 How do you ensure that the privacy policy of the third-party website and/or application is reviewed to ensure that it appropriately supports the USAID privacy protection position?

Not Applicable.

3.9.3 If you have a link from USAID.gov to this third-party website or other location that is not a part of an official government domain, do you provide an alert (such as a statement or "pop-up") to visitors explaining that they are being directed to a non-governmental website that may not afford the same privacy protections as USAID?

Not Applicable.

3.9.4 If you incorporate or embed the third-party application on the USAID website, how do you disclose to the public the third-party application?

(If you choose Yes*, please describe the disclosure.)*

Not Applicable

3.9.5 How do you create the appropriate USAID brand to indicate an official USAID presence on the third-party website, and how you distinguish USAID activities from those of non-governmental actors?

The application is branded in accordance with ADS 320 and supplemental USAID branding policies.