United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Enterprise Identity and Access Management (EIAM)	
Preparer: Olamide Akinbobola (FED); Oliver Petruzel (CTR)	**Office:** OMS/ITSSS/OITO
Date: 01/23/2020	**Phone:** (202)566-2538
Reason for Submittal: New PIA____ Revised PIA____ Annual Review_X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).	

Provide a general description/overview and purpose of the system:

The Enterprise Identity and Access Management (EIAM) system is a collection of standard based commercial off the shelf (COTS) Identity Access Management (IAM) products and suites which provide enterprise authentication and authorization services for the agency. EIAM consist of Web Access Management (WAM), Directory Administration, Identity Governance, and Enterprise Identity Data Warehouse (EIDW). **The only components that contain any PII is WAM (WAA self-registration) and EIDW.**

WAM is a key component of the EPA Enterprise Identity and Access Management Architecture. WAM is a directory service for the agency and provides enterprise authentication services. WAM services include:

- Single web application directory to support web applications containing all web application users
- Authentication & Authorization for web applications, GSS Unix Environment, and the HPC Unix Environment

- WebGate
- Access policies
- Workflow approvals
- Audit information
- Web Single Sign On (SSO) for WAM protected applications
- Password expiration warnings (External Only)
- External User Registration

WAM infrastructure consist of the below technology:

Oracle Unified Directory – OUD formerly known as (Oracle Identity Directory-OID) provides a Web Application Directory which applications can leverage. The OUD offers comprehensive and flexible support for directory access control. This includes entry level, attribute level, and prescriptive access control to provide varying levels of security to custom fit enterprise and service provider needs. An administrator can grant or restrict access to a specific directory attribute, entry, group, or naming context. The OUD implements three levels of user authentication: anonymous, password-based, and certificate-based using Secure Sockets Layer (SSL) v3 for authenticated access and data privacy.

OUD offers sophisticated password policy management capabilities (e.g., control over expiration times and password length) and the ability to store passwords using a variety of hashing schemes. These features allow administrators to define consistent security policies across applications and easily share passwords with other systems. The current configuration provides for the authenticating of the password to eDirectory. For this reason, EPA Staff and on-site business partners cannot change their password from within Web Application Access.

Oracle Access Manager - OAM is a Web interface provided by Oracle to manage the user information stored in OUD. Through the OAM console, system administrators directly manage user information and group membership. System owners are still restricted to only change user information for users for which they are the authoritative source. If they attempt to change user information for a user created through the directory synchronization scripts, the information will be overwritten the next time the synchronization scripts are run.

Web applications interested in managing user information through OAM are identified at the creation of the design meeting for any Web application. Access to OAM is approved by the System Owner and only EPA employees and internal affiliates are allowed access to manage their users.

Identity Governance:

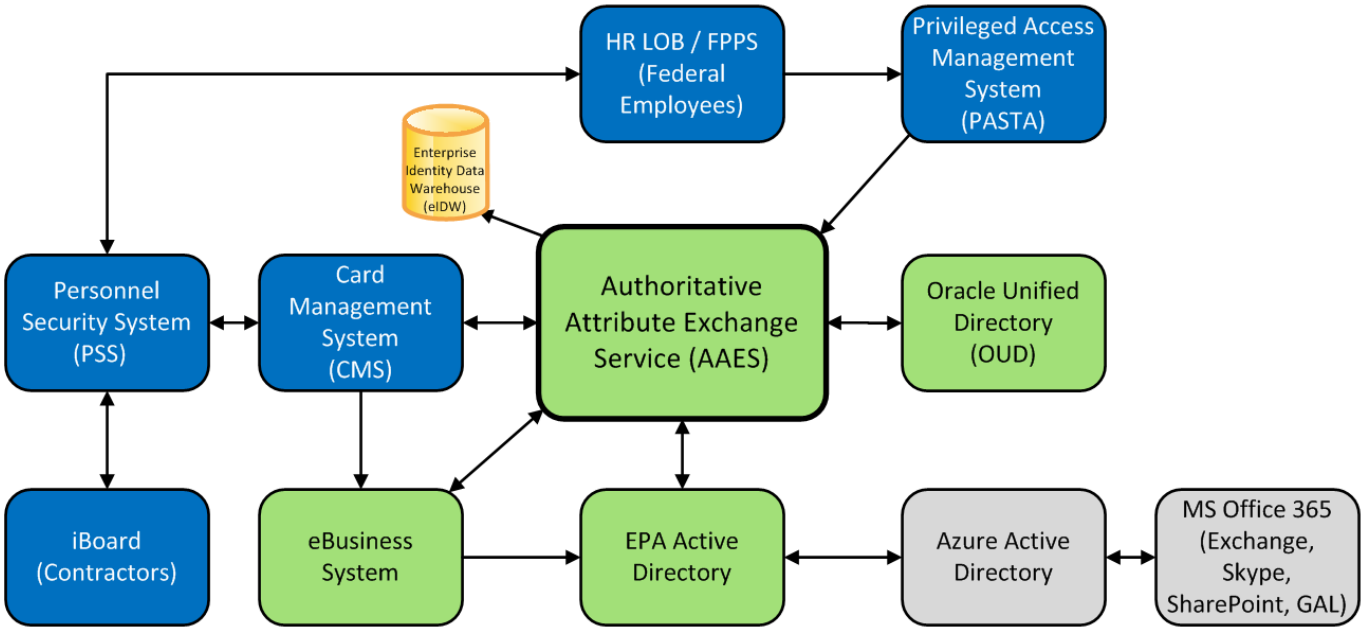
Oracle Identity Manager (OIM) is a Governance solution that provides self-service, compliance, provisioning and password management services for applications residing on premise or on the Cloud. Manages identities and access privileges for employees, business partners, and external affiliates.

Oracle Identity Manager makes it possible for enterprises to manage the identities and access privileges of their customers, business partners, and employees, all on a single platform. It allows these users to manage their own identities as well as those of others by using delegated administration. It allows enterprises to setup delegated administrators, who are users empowered to manage the identities, passwords, password policies, and access of other users. Business users can create and manage the lifecycle of enterprise roles, which grant access to end-users. These roles can be granted automatically by using rules. With the help of roles and access policies, organizations can ensure that their users are on-boarded and off-boarded in a timely and automated manner.

Enterprise Identity Data Warehouse – uses OIM for the authoritative attribute exchanges services. EIDW is the technical solution that provides the Agency with the capability to connect various authoritative data sources and share the attributes with shared enterprise infrastructure. Authoritative identity attribute sources are leveraged by the

Enterprise Identity Data Warehouse (EIDW) in alignment with the Federal Identity, Credential and Access Management (FICAM) Roadmap for Digital Identity Service. The roadmap initiative #5: Streamline Collection and Sharing of Digital Identity Data is accomplished with EIDW. This allows the agency to eliminate identity silos and reduce operating costs. It also provides automated provisioning and de-provisioning and greater auditing capability.

Diagram of the current systems integrating with EIDW for authoritative attribute exchange services:



SecureAuth- (shibboleth) provides EPA's One Time Password solution for Multi-Factor Authentication for non-PKI authenticated users.

Active Directory Federation Services – Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity. It is currently used at EPA to provide authentication to MS Office 365 in the Microsoft government cloud.

Claims-based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims-based authentication.

In ADFS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

In practice this approach is typically perceived by the user as follows:

- The user logs into their PC.

- The user needs to connect to MS Office 365.
- The user navigates to MS Office 365 via EPA's My Workplace site.
- MS Office site does not require any password to be typed in - instead, the user credentials are passed to the site using ADFS.
- ADFS integrates with Active Directory Domain Services, using it as an identity provider. ADFS can interact with other WS-* and SAML 2.0 compliant federation services as federation partners.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- Federal Information Security Modernization Act of 2014 (FISMA, 44 U.S.C. § 3541, et seq);
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, July 26, 2016;
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007;
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, "Minimum Security Requirements for Federal Information and Information Systems," August 2013; and
- Homeland Security Presidential Directive 12 (HSPD-12), "LincPass", August 12, 2004
- NIST Special Publications (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.
- Additional programmatic authorities may apply to maintenance of the credential.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

EIAM has an Authority to Operate (ATO) that will expire in February 2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service

(PaaS, IaaS, SaaS, etc.) will the CSP provide?

The data will not be maintained or stored in a cloud.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

WAM and EIDW connect to other agency authoritative sources to pull information on EPA employees and Internal Affiliates for authentication and authorization to agency resources.

WAM (Self-registration) component collects information for external partners with whom the Agency conducts business and not for public users. The system collects the below information from the business partners for use to make an assumption of their identity for application owners that use WAM for authentication. The self-registration automatically creates a unique User ID (UID) for the external partner when the application owner approves the requests. The email is used to send emails about password expiration to the external partner. The application owner is responsible for approving or rejecting the access request that is submitted via the self-registration form. OUD maintains the external partner data and passwords.

WAA
User First Name
User Last Name
Business email
Business Phone Number
Business Mailing Address

EIDW component consumes the following information from the following systems (table below):

eBusiness
User Legal First Name
User Legal Last Name
User Legal Middle Name
User Preferred Name
Affiliation
Employee Common Identifier/Workforce ID
Organization Code
Organization Name
Office Telephone Number
GFE Cell Phone Number
Official Title
Primary COR Name
Contract Number
Contract Status

Active Directory
User Principal Name
LAN ID
Email

Card Management System
PIV Distinguished Name
Issuer of Certificate
PIV Public Certification

PASTA
Employee Supervisor Name

2.2 What are the sources of the information and how is the information collected for the system?

WAM: The information is from the external business partner completing the electronic self-registration form. The individual requesting access submits a self-registration form electronically and the individual application owner is responsible for ensuring the accuracy of the information.

EIDW: The information is consumed by the system interconnections from eBusiness, Active Directory, Card Management System (CMS), and PASTA.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

EIAM does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

WAM self-registration form has a level of assurance 1 and the external business partner requesting access supplies the information. The data accuracy is the responsibility of the EPA Sponsor/Application owner to verify.

EIDW: Person data for employees and contractors is pulled from source systems managed by ORAM, OARM is the system owner for Human Resources, Personnel Security and Physical Access.

WAM and EIDW are only available to authorized users within the secure EPA network. It is not accessible by members of the public. The only availability is the self-registration form that contains no information until completed by the individual and once the electronic form is submitted the information is not viewable. The self-registration form is only for external business partners.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Risk associated with characterization of EIAM information could be a potential leakage of information and a risk of the system being hacked.

Mitigation:

Encryption mechanisms prevents information loss or theft while it is stored in the underlying database files. All data is encrypted in transport and at rest. This prevents data from being readable while stored in database files, backup files, and exported LDIF files. These are encoded using Salted SHA-512 (SSHA-512) algorithm.

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

The system offers a number of mechanisms to secure access to data, such as access control rules, password authentication, and SSL. Non-privileged users are prevented from executing privileged functions and mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges. Restricting non-privileged users also prevents an attacker who has gained access to a non-privileged account, from elevating privileges, creating accounts, and performing system checks and maintenance. Authorized users are required to have a PIV card for access.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

An access control document does exist with standard operating procedures in place on the EPA SharePoint drive that exist entitles EPA Active Administrators Guide that details the following access controls:

Active Directory (AD): AD systems are only accessed by users identified and selected to support organizational /business functions.

- AD has designated account managers for each system.
- Each AD system has established conditions established for each user role and or group membership.
- Each account that has access to any AD system must be authorized, has a defined role and group membership and actions taken can be tracked. There are no guest/anonymous or temporary accounts with AD systems.
- Before creation of accounts for AD systems, proper approvals must be granted.
- Account creation, access, modification, etc. is made in accordance with EPA standards.
- The use of accounts used to access AD systems are monitored either within the system or by a secondary tool.
- Managers of each AD system is notified when users are terminated or transferred by email, or when the individual usage or needs changes by the supervisor/manager of the individual.
- Access to AD systems need to be authorized, needs to have a valid "need to have access" associated with the EPAs organizational or business functions.
- Review of user accounts are done, but there is no set time frequency.
- There are no group or shared accounts for AD systems.

Account management for Identity Governance is handled at the enterprise level. Identity Governance relies upon Active Directory for user account management and identification and authentication services. Users must have an EPA domain account prior to being able to gain access to the application.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. The system protects confidentiality and integrity of data at rest through a number of controls, including restricting read-only or read-write access to data to users whose roles permit such actions, limiting file permissions and database access rights consistent with a least-privilege model.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

ITS-EPA III contractors have the 40 CFR part 16 [FAR Clause] within the contract with EPA in support of EIAM. Each contractor is required to sign an ITS-EPA III Contractor Computer User Agreement upon hire which outlines the Rules of Behavior, Acceptable Use, Conflict-of-Interest, and Nondisclosure policies in the use of EPA equipment and resources. Any ITS-EPA III contractors that use EPA Remote Administration for server access must all sign a similar User Agreement. EPA Privacy Act procedures described in the Privacy Act Regulations at 40 CFR part 16 are included within the system support contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The information that is collected is retained for the life cycle of the digital identity that is issued from and contains the information. The digital authentication of subjects to systems over networks specifically and not addressing physical access. The information is used for identity and access management. EIAM follows EPA Records Schedule 0089 Information Tracking System and 1012

Information and Technology Management.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Risk associated with information leakage is where EIAM could reveal sensitive data, such as technical details of the application, environment or user specific data.

Mitigation:

The appropriate records control schedule is strictly followed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No, information is not shared outside of EPA.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. No information is not shared externally.

Mitigation:

N/A

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

5.1 How does the system ensure that the information is used in accordance with stated practices in this PIA (Section 6.1)?

EIAM ensures that the information is used for its intended purposes by limiting access to the information collected. There are numerous controls in place to ensure data integrity and to prevent unauthorized access. Access is controlled by User Roles, each role assigned gives access only to the data he/she needs to perform their job. The data is stored in the Data Tier Servers running at the EPA NCC RTP location. This is an Oracle relational database. The data tier contains the Identities, Roles, Groups, Access/Permissions, Policies, Workflows, notifications, scheduled tasks, and entitlement attributes. All the data is encrypted per the protocol used for the particular Directory and Data Tier.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Employees and contractors take the EPA Annual Information Security and Privacy Awareness Training. All users are required to read and sign the EPA Rules of Behavior that governs the appropriate use of information systems.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Risk associated with auditing and accountability in relation to EIAM would be unauthorized access to audit records that are maintained.

Mitigation:

Encryption mechanisms prevents information loss or theft while it is stored in the underlying database files. All data is encrypted in transport and at rest. This prevents data from being readable while stored in database files, backup files, and exported LDIF files. These are encoded using Salted SHA-512 (SSHA-512) algorithm.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

OUD is a Lightweight Directory Access Protocol (LDAP) compliant directory service that aggregates user credential information. The information from the self-registration form is used to create a unique digital identity within an identity directory. OUD is a centralized user identity store. The owner of the application uses the information completed on the self-registration to help determine which external individual(s) to give access to and what level of access(authorization) to their system. WAM supplies the authentication, more simply the entry to the application, and the application owner specifies what the person has access to once they are permitted access to the application.

OIM is Oracle's standalone identity management solution for EIDW. It provides User Administration, Workflow and Policy, Password Management, Audit and compliance Management, User Provisioning and Organization/role management functionalities. Allows EIDW to manage the integration of the data collected by EIDW from authoritative sources to share identity information in an automated fashion for provisioning and de-provisioning of users, eliminates manual entry of identity data for integrated systems, and establishes a component service of the Federal Identity, Credential, and Access Management (FICAM) services framework for digital identities. Meets FICAM #5 roadmap for streamlining collection and sharing of digital identity data within the Agency.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_No. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

Because there are three protocols for communication (SCIM API, SQL Net Protocol, and LDAP) the primary data elements used to retrieve EIAM information are the following: the LANID (sAMAccountName in AD, User Name in EIDW and OUD) on a single user.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EPASS EPA-62 R

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Risk are in association of unauthorized uses of information. Unauthorized purposes may include gaining

access to information/data, system accounts, etc.

Mitigation:
Encryption mechanisms prevent information unauthorized access as well as loss and theft while it is stored in the underlying database files. All data is encrypted in transport and at rest. This prevents data from being readable while stored in database files, backup files, and exported LDIF files. These are encoded using Salted SHA-512 (SSHA-512) algorithm.

All the system components for WAM and EIDW are hosted at the NCC in RTPNC and PTY on the internal EPA Network. WAM and EIDW are only accessible to authorized users.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

WAM and EIDW are internal applications and only accessible by authorized individuals. EPA employees and contractors are required to take the EPA Annual Privacy and Information System Awareness training. Training is conducted for each functional role and the Rules of Behavior that is signed contains the list of standards governing the appropriate use of the information system. Prior to authorization to these systems the Rules of Behavior must be read and signed.

The WAA page that provides the self-registration form link has a privacy warning notice and links to the EPA Privacy and Security Notice. The notice states that:

1. Users are accessing a U.S. Government information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use is prohibited and subject to criminal and civil penalties; and
4. Use indicates consent to monitoring and recording.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

There is a consent confirmation box that is mandatory for submitting the self-registration automated form. They can cancel the self-registration if they choose not to accept the Privacy & Security Policy.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

None. The purpose to notify them that they are using an EPA resource and only authorized users are allowed access. The email is collected to send confirmation emails to the business partner completing the form. The name is required to verify identity and create a unique ID to gain access to the requested application.

Mitigation:

If the individual declines the notice, then they will not be able to submit the self-registration request and will not be granted access to the EPA application using WAM for authentication.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

The External Business partner can login to the WAM WAA web interface and access their Profile information at any time. They are only allowed to view the information with the exception of being able to manage their password. EPA employees and Internal Affiliates are not managed by WAM.

EIDW information is not accessible by individual users.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Comments and request for correction can be made by requesting directing comments to Docket ID EPA-HQ-OEI-2012-0836 either electronically in www.regulations.gov or in hard copy at the OEI Docket, EPA/DC, EPA West Building, Room 3334, 1301 Constitution Ave. NW., Washington, DC. The Public Reading Room is open from 8:30 a.m. to 4:30 p.m., Monday through Friday excluding legal holidays.

8.3 How does the system notify individuals about the procedures for correcting their information?

Comments and request can be made by requesting directing comments to Docket ID EPA-HQ-OEI-2012-0836 either electronically in www.regulations.gov or in hard copy at the OEI Docket, EPA/DC, EPA West Building, Room 3334, 1301 Constitution Ave. NW., Washington, DC. The Public Reading Room is open from 8:30 a.m. to 4:30 p.m., Monday through Friday excluding legal holidays.

8.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

There is no risk associated with the redress. There are procedures in place to review the data that have been communicated to individuals through procedures outlined in the SORN and FOIA processes.

Mitigation:

None.