United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 08/2018)
(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: Smart Mobile Tools for Field Inspectors

Preparer: Lauren W Jones	**Office: OECA**
Date: July 18, 2019	**Phone: 202-564-0389**

Reason for Submittal: New PIA ✓ **Revised PIA**____ **Annual Review**____ **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:

Smart Tools is a commercial off the shelf (COTS) application used for the collection of field observations and evidence during inspections of EPA/State regulated entities. Its purpose is to replace the standard, hard copy, hand written collection of field notes and observations (i.e. green notebook) and to consolidate the storage of those field notes with electronically collected evidence about a regulated entity. Inspection data elements that are collected in Smart Tools will be pushed from Smart Tools into appropriate Systems of Record (i.e., RCRAinfo, ICIS) to automatically create inspection records within those SORs. These SOR's do not collect privacy information and, therefore, do not have a System of Record Notice (SORN) associated with them. Use of Smart Tools is by invitation and only available to EPA personnel, Inside Affiliates, and External Affiliates (partners) and is not publicly available. Jointly governed by EPA, ECOS and other program associations, Smart Tools fundamentally improves the operation and management of environmental inspection programs.

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?

RCRA Section 3007, 42 U.S.C. 6927

CWA sections 301(a), 304(h), and 501(a); 33 U.S.C. 1311(a), 1314(h), 1361(a).

CAA, 42 U.S.C. §7401 et seq. (1970)

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?

Development of a system security plan (SSP) is currently underway and is not yet completed, as of April 2019. An ATO is being targeted for September 2019. ATO expiration date is not applicable.

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.

The information is not covered by the Paperwork Reduction Act since the information is collected as part of investigative activities and is requested of a single entity.

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?

No

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).

The system will collect: First Name, Last Name, Email, Phone number of individuals involved in an inspection, as well as the Facility Name, Facility Address, Facility ID, Facility Personnel First Name, Last Name, Phone number, email address

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

The Smart Tools application relies on EPA services provided by WAM (external) and EIDW (internal) as the authoritative sources to pull authentication information on EPA personnel, Inside Affiliates, and External Affiliates (partners). WAM (Self-registration) component collects information for external partners with whom the Agency conducts business and is not for public users. External Affiliates using the system will self-register their name, email, phone number in WAM. EPA personnel and Internal Affiliate authentication data will be retrieved from EIDW. Users will retrieve the Facility Name, Facility Address, and Facility ID from RCRAinfo. Names, phone numbers, and email addresses of facility staff will be collected and entered into the system by the inspector during the on-site inspection. The type of inspection is identified and entered by the inspector.

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

No, Not applicable.

2.4 Discuss how accuracy of the data is ensured.

Access to Smart Tools application is by invitation only. Smart Tools Admin will invite both EPA and State users via a secured link. State users (External Affiliates) will have to register for an Account in WAM using the same email address at which they received the invitation. 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 EPA employees and Internal Affiliates is pulled from source systems managed by OMS, OMS is the system owner for Human Resources, Personnel Security and Physical Access. EPA personnel and Internal Affiliate data was verified during their onboarding process. Facility information comes from EPA's Facility Registration System (FRS) which has its own assurances for data accuracy. The accuracy of facility data is inherited from FRS. All other manually entered data is spell checked and verified by the user.

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:

Smart Tools authentication relies on WAM and EIDW. WAM and EIDW are only available to authorized (by invitation) users within the secure EPA network. Smart Tools 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. EPA personnel and internal affiliate names, email addresses, and phone numbers are provided by EPA EIDW infrastructure. Names, email address, and phone numbers of facility personnel are provided by the individuals and entered in to Smart Tools by the application user. All data within Smart Tools is encrypted

Mitigation:

All users of Smart Tools are required to take Information Security training annually. The IT Rules of Behavior must be read and signed.

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?

Yes. The system offers several 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 EPA and Internal Affiliate users are required to have a PIV card for access. External Affiliates will utilize a username/password combination as factor 1 and a One Time Password (OTP) for factor 2 for system 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?

The system uses role-based access authorization. Logical access controls are employed to permit only authorized access to the system and restrict users to authorized transactions, functions, and data. These automated controls ensure that only authorized individuals gain access to Smart Tools resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable for their actions. These controls support the separation of duties principle.

Smart Tools uses information from WAM/EIDW for authentication. Personnel having authorized access to WAM/EIDW include the System Administrators that manage WAM/EIDW. System Administrators that consume the attributes from WAM/EIDW for Smart Tools have a view of the attributes available and do not retrieve the information specifically on a person. Credentials are obtained from the WAM/EIDW authentication servers to identify the user to the Smart Tools application. This authentication traffic is encrypted to ensure that no data is passed in the clear. FRS data identifies the facility for the inspection record. All other collected information is used in the inspection record to identify participants.

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

Yes. 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?

EPA staff, EPA Contractors for media programs, and State regulatory personnel will have controlled access to data in the system. Each entity (EPA, State) will have access only to the data that they have entered into the system. Access to the data will further be controlled down to the individual as well as by role. Contractors are required to sign a Smart Tools 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 Smart Tools contractors that use EPA Remote Administration for server access must all sign a similar User Agreement.

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 collected for identity and access management in WAM and EIDW are retained for the life cycle of the digital identity that it is issued from and contains the information. This information is governed by EPA Records Schedule 0089 Information Tracking System and 1012 Information and Technology Management. Identity and access management data will be eliminated according to EPA policy for record retention as documented in EPA Records Schedule 704 Personnel Security Case files. The retention schedule for inspection data within Smart Tools will depend on the statute and whether the records become part of an enforcement action. This type of data is governed by Records Schedule 1044. http://intranet.epa.gov/records/schedule/final/1044.html

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:

There are no risks associated with retaining the information as long as the individual is employed with the EPA or with a state agency partner.

Mitigation:

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.

Most of the information collected in the system will not be shared outside of EPA. The only information commonly shared is the final inspection report which is created outside of Smart Tools that has been reviewed and approved, signed, converted to PDF and imported back into the system. Inspection reports are commonly shared outside of EPA in the normal course of business and only include the inspector(s), manager(s), and facility personnel name(s), and titles. No email addresses or phone numbers are associated with any name of personnel identified in the inspection report. Facility data collected in the system is already public information gathered from the Facility Registration System (FRS), Enforcement and Compliance History Online (ECHO), or RCRAinfo. It is common practice to send this to the facility and the state agency in the state in which the inspection occurred. EPA in the near future will post these inspection reports to the web and associate them with the facility data found in ECHO. There are no restrictions on how the inspection report is used.

4.2 Describe how the external sharing is compatible with the original

purposes of the collection.

EPA routinely transmits final inspection reports to the state and the regulated facility as part of the inspection process. Digital sharing of the final inspection report using smart tools is no different than what occurs today in the analogue world.

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?

There are no sharing agreements or MOUs associated with the data in the system. Access is by invitation only and provisioned by a system administrator. Uses of the information is limited to the entity creating the data, state or EPA, and there are no restrictions on the use of that information by the respective regulatory entity.

4.4 Does the agreement place limitations on re-dissemination?

As there are no agreements, there are also no limitation on the use of the information by the entity that created it.

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:

There are no risks associated with sharing the final inspection report between partners and the facility.

Mitigation:

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?

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. User authentication 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. Authorization data is stored in Data

Servers running at the EPA NCC RTP location. This is a Microsoft SQL relational database. The data server contains the unique user ID for WAM/EIDW authenticated users as well as the user role, access/permission, and policies. All the data is encrypted per EPA protocols and policies.

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

EPA personnel and internal affiliates (contractors) are required to undergo annual privacy act and information security awareness training. Prior to system access, external affiliates (states) would be required to undergo training equivalent to EPA requirements. 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:

The Privacy and Security Awareness training are run by the Privacy and Security programs. These program offices ensure compliance with training and policies supporting these programs.

Mitigation:

N/A

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.

The information from the self-registration form is used to create a unique digital identity within an identity directory. 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.

EIDW manages internal user data that is collected from authoritative sources to share identity information in an automated fashion for provisioning and de-provisioning of users, eliminating manual entry of identity data for integrated systems, and establishing a component service of the Federal Identity, Credential, and Access Management (FICAM) services framework for digital identities. EIDW meets FICAM #5 roadmap for streamlining collection and sharing of digital identity data within the Agency.

On-site collection of facility personnel information is collected during the opening conference of an inspection. This data is provided by the individual and entered into the inspection record by the Smart Tools user. This data is used to identify individuals participating in the inspection and as a means to contact those individuals in the future if questions regarding the inspection or observations need clarification prior to making a regulatory compliance determination.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes__ No__X_. 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.)*

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

None

6.4 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

The WAM self-registration blank form link is available to those that are given the URL (invited) but contains no information and is only for use by External Affiliates (state partners) and is not for general public use. Authentication is required to log-in.

The EPA will collect personal information to identity Smart Tools users in order to create a Unique Identifier and verify business purpose for access. The personal information includes the name, phone number, and email address of the application user. The self-registration form will not request a Social Security number, date of birth, address, description of physical appearance, medical information, or job description. The information that is stored in the database will be used to grant you access to agency-controlled information systems or applications. EPA will use the information collected for security purposes and to verify access to agency-controlled information systems or applications.

Mitigation:

Identity attribute encryption 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. WAM/EIDW data files, backups and LDIF files are encoded using Salted SHA-512 (SSHA-512) algorithm. Smart Tools uses AES symmetrical key encryption for all sensitive data stored in the database. SSL and secure HTTPS protocol is used between client and the web server. This protocol creates a secure channel, provides encryption, and secures identification of the server. This protocol requires a certificate that must be signed by a trusted authority. All communication between the web server and the application layer happens through the Asp.net Web API Restful Services. EPA Smart tools enables Token Based authentication; each request will have signed token as part of request header. All connections made to and from Smart Tools are made using TSL encryption. Data in rest and in transit is encrypted using FIPS-140-2 compliant encryption technologies.

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

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. Additionally, multiple levels of security are maintained by the system's access controls. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users of the system are given unique personal identifiers, and all interactions between the system and the authorized individual users are logged.

*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.

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?

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:

Mitigation:

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?

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

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

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:

Mitigation: