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: AutoAudit for Windows (AAW)	
Preparer: Frank Fennell	**Office: OIG**
Date: 4/2/2020	**Phone: 202-566-2697**
Reason for Submittal: New PIA____ Revised PIA_X___ 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:

AutoAudit for Windows (AAW) is a COTS application that provides the ability to manage the audit activities required as part of the EPA OIG business processes. The application supports nationwide audit work at EPA OIG for headquarters and regional offices. It is accessed via government furnished equipment (GFE) laptops and desktops. The OIG uses AAW for performance, financial-related, financial statement audits and reviews, and evaluations

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?

EPA Office of Inspector General (OIG) mission and goals pursuant to the Inspector

General Act of 1978, 5 U.S.C. app. Refer to SORN EPA-50 (AutoAudit).

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?

Yes, AAW does have an SSP. A temporary ATO has been approved and will expire on November 15, 2019.

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?

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 EPA OIG uses AAW to report on the efficiency of EPA programs and operations. The OIG provides independent audit, evaluation, investigative and advisory services that promote economy, efficiency and effectiveness; and help to prevent and detect fraud, waste and abuse in order to add value in EPA programs and operations. The OIG has further interpreted this statutory mission through its strategic and annual performance goals for contributing to environmental quality, human health and good government to inspire public confidence in the integrity of EPA operations.

OIG auditors and evaluators use AAW to create, update, review and store documents related to their specific job assignment. These documents consist of working papers, manager comment sheets, audit reports and other documents used during the audit process. AAW categorizes these documents for retrieval and storage. Examples of the data elements captures in the workpapers include names, work phone, date of birth, email, cell phone number, and Audit Documents Awards.

See SORN EPA-50.

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

EPA Program Offices, EPA Employees, and EPA Contractors/Agents are the sources of information. The information is collected from interviews and research performed. The auditors or evaluators input the data into stored electronic fields and forms in the AAW application.

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

Not directly. The auditors, evaluators and investigators may store information from commercial sources or publicly available data during their audit or investigation. The information is used as supporting documents as part of their audit or evaluation.

2.4 Discuss how accuracy of the data is ensured.

AAW is programmed with input field validation. A text field must contain text data and date fields must contain date data. In addition, the managers review the data for accuracy prior to making decisions.

The OIG has a data quality policy (OIG Policy 004) that ensures proper management responsibilities are in place to comply with the EPA's Information Quality Guidelines (OMB Section 515).

Annually, the OIG Deputy Inspector General certifies as a part of the OIG Annual Performance Report that all data reported through OIG information systems meet the EPA data quality standards.

OIG ensures that information is relevant, accurate, timely and complete.

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:

There are risks associated with unauthorized access or disclosure of information or inaccurate data.

Mitigation:

AAW is an internal application used by EPA OIG employees only. Only staff with a need to use the system are provided access.

Users must read an AAW Rules of Behavior document and return a signed Security Awareness form prior to gaining access to the system.

Users must have an AUDITOR SETUP record created and configured in the application to gain access to the system. In addition, there are separate requests to increase the user's privileges with different levels of access and permissions implemented inside AAW.

Authentication to the system occurs through the agency's Active Directory Domain Controller. A user must have a strong password (combination of alpha-numeric-symbolic of at least 12 characters in length) that are changed a minimum of every 60 days. Also, all devices that connect to the system use a screen lock; both (screen lock and password) are enforced by agency policy.

Additionally, all users must take annual mandatory Security Awareness and Privacy training as provided by the agency.

Security controls are implemented and reviewed annually.

Continuous Monitoring Assessments (CMAs) are conducted annually

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, AAW has access control levels implemented. It will only allow access to individuals in order accomplish their job.

Additionally, there is a 'Confidential' feature within the system. Any audit designated as 'Confidential' is restricted to only those staff members listed for the audit.

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

Access controls are documented in the CIO policy and procedures, CIO 2150-P-01.2. The specific procedures are documented in the AAW System Security Plan (SSP) for the AC-6 controls. Requests to access the system must be submitted via a ticket system by the user's supervisor or higher-level manager in the directorate chain to annotate approval to access the system. Additionally, requests to increase the user's privileges must be submitted via a ticket system by the user's supervisor or higher-level manager.

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

Yes, each ASSIGNMENT in the application has its own access control levels to further restrict and manage the security of the system.

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?

Only OIG employees will have access to the information system; no external parties or non-OIG personnel have access to the system.
Yes, it included contractors who work for OIG. SAIC has their own onboarding process and includes non-disclosure agreements as well as agency FAR clauses.

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.

Information is retained based on legal and federal requirements as described under the **Inspector General Act of 1978, as amended, U.S.C. app.. AAW uses the** EPA Record Retention Schedule 1016 (audits, evaluations and investigations).

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 risks of storing data past the retention schedule or reviews not performed to identify data to be retained or destroyed.

Mitigation:

An annual review of the information against the applicable RECORD SCHEDULE of the audits maintained in the system is performed. Audits past their authorized retention date are deleted from the system. A review is then performed to confirm that the information has been removed.
.

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 shared outside of the EPA OIG.

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

Not applicable (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?

Not applicable (N/A)

4.4 Does the agreement place limitations on re-dissemination?

Not applicable (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. Information is not shared externally.

Mitigation:

None.

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)?

As documented in the AAW System Security Plan (SSP for the Monitoring and Auditing (AR) controls, the OIG Program Office utilizes the Risk Management Framework

strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. AAW is subject to annual third-party security assessments conducted by FAA. AAW team members perform regular reviews of login auditing to monitor access. It is also the Office of Inspector General's (OIG) responsibility for monitoring and auditing privacy controls and internal privacy policies on a continuous basis to ensure effective implementation of this procedure.

Additionally, the agency Privacy Office conducts annual reviews to evaluate the PII data collected and inquires whether PII data is still required. OIG responds to these annual FIS data calls that are used to determine if the collection of PII is relevant and necessary to accomplish the mission. These data calls assist in ensuring data collected and retained is for the specific documented purpose. In response to the FIS data call, the OIG re-evaluates the information collected and validates the need for that information.

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

All EPA OIG staff take mandatory annual Information Security and Privacy Awareness Training.

Additionally, when working in AAW, if a specific document contains PII, teams have been directed to label the electronic file as containing PII. Staff have been instructed to include a statement at the beginning of the working paper in large letter "Contains PII". (Exact wording varies by team).

The policy and procedure that staff follow regarding labeling of PII is OIG Procedure 413.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Yes. There is minimal risk related to auditing and accountability changes to the configuration of the system.

Mitigation:

The agency Privacy Office conducts a review (Privacy Impact Analysis) to evaluate the PII data collected and reviews whether certain data are still required.

OIG responds to the annual FIS data call that we are only collecting PII relevant and necessary to accomplish the mission.

Data is only collected and retained for the specific purpose.

AAW is a restricted application available to only EPA OIG government employees.

Only authorized OIG administrators can effect changes to the configuration of the system.

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.

In pursuant of the Inspector General Act of 1978, the OIG conducts independent audits, evaluations, investigations and advisory services that promote economy, efficiency and effectiveness; to prevent and detect fraud, waste and abuse in EPA programs. AAW is the application the auditors and evaluators use to store and report on the data they collected.

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.)

The information is primarily accessed and retrieved by an assignment audit number.

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

SORN EPA-50.

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:

There are risks associated to unauthorized access, uses or disclosure of information.

Mitigation:

OIG employees read, understand and accept the Rules of Behavior. If they decline, they will not have access to AAW. In addition, each time the user uses AAW the user is presented the OIG Systems Warning Notice that communicates system monitoring each time a user accesses the system (see below). The user is then prompted to either Agree or Decline.

OIG Systems Warning Notice:

In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:

1. you are accessing U.S. Government information and information systems that are provided for official U.S. Government purposes only;
2. unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative, or other lawful action;
3. the term U.S. Government information system includes systems operated on behalf of the U.S. Government;
4. you have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems;
5. at any time, the U.S. Government may for any lawful government purpose, without notice, monitor, intercept, search, and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems;
6. at any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information;
7. any communications or information used, transmitted, or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including but not limited to, administrative purposes, penetration testing, communication security monitoring, personnel misconduct measures, law enforcement, and counterintelligence inquiries; and
8. you may not process, or store classified national security information on this computer system.

OIG users also take annual security training and for those with privileged access, at least two role-based security training per year. Regular users sign off on the Rules of Behavior document while those with Privileged access complete the Privileged User Rules of Behavior.

*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.

.

Program offices and individuals are contacted as part of the OIG audit and evaluation process, documented in OIG Policy and Procedure 101, Project Management Handbook for Audit. Information is provided under the authority of the Inspector General Act of 1978, as amended, U.S.C. app.. Further, EPA Audit and Evaluation Manual (Manual 2750) directs EPA staff to provide the OIG with access to records.

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?

Information is requested and individuals are expected to provide information under the authority of the Inspector General Act of 1978, as amended, 5 U.S.C. app.. An option to consent or decline providing this information is not provided by the auditor or evaluator.

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. There are clearly defined procedures in the SORNS that discuss records access and contesting records.

Mitigation:

None.

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?

AAW data is not accessible by the public. Record access procedures are published via SORN.

To the extent permitted under the Privacy Act of 1974, 5 U.S.C. 552a(k)(2), this system has been exempted from the provisions of the Privacy Act of 1974 that permit access and correction. However, the EPA may, in its discretion, fully grant individual requests for access and correction if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect. The exemption from access is limited in some instances by law to information that would reveal the identity of a confidential source. Requesters will be required to provide adequate identification, such as a driver's license, identification card or other identifying document.

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

The procedures are as stated in the Federal Register notification for SORN EPA-50. Requests for correction or amendment must identify the record to be changed and the corrective action sought by completing EPA Privacy Act request procedures set out in 40 CFR part 16.

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

This information is stated in the Federal Register for SORN EPA-50.

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:

None. There are clearly defined procedures in the SORN that discusses records access and contesting records.

Mitigation:

None.