PRIVACY IMPACT ASSESSMENT

Submit in *Word format* electronically to: Linda Person (person.linda@epa.gov)

Office of Environmental Information

System Name: The Inspector General Enterprise Management System (AUTOAUDIT)

Preparer: Jaime Aguilar	**Office: OIG**
Date: 01/2016	**Phone: 202-566-2694**

This project is in the following life cycle stage(s):

Definition ☐   Development/Acquisition ☐   Implementation ☐

Operation & Maintenance ☒   Termination ☐

Note: Existing Systems require an updated PIA when there is a significant modification or where changes have been made to the system that may create a new privacy risk. For a listing of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f) at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.aspx

I. Data in the System

1. What data/information will be collected/contained in the system? Audit related data

2. What are the sources and types of the data/information in the system?

   The AutoAudit application has data fields (rich text) that allows EPA OIG employees to attach files of all kinds within the AutoAudit application.

3. If the system has been modified, are the original personally identifiable information (PII) elements still being collected or contained in the system? If no, what are the elements currently being collected? When did the collection of the original PII elements stop? How was the old data removed from the system?

   Original PII information from audits are maintained in the AutoAudit application. The data is archived in its native form in a Lotus Notes – AutoAudit application.

4. How will the information be used by the Agency?

Data is used to support EPA OIG mission and goals and in pursuant of the Inspector General Act of 1978.

5. Why is the information being collected? (Purpose)

The EPA Office of Inspector General (OIG) uses the AutoAudit application 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 in order to inspire public confidence in the integrity of EPA operations.

OIG auditors and evaluators use AutoAudit 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. AutoAudit categorizes these documents for retrieval and storage.

II. Access Controls for the Data

1. To ensure user authentication, does the system have limited login attempts or require security question answers? If yes, when the user becomes locked out how will they gain access to the system?

No, the Lotus Notes application that AutoAudit is programmed does not lock after limited login attempts.

2. How often are passwords required to be changed?

Passwords are required to be changed every 90 days based on the agency's policy.

3. Who will have access to the data/information in the system *(internal and external parties)*? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

EPA OIG employees have access to the data based on their position on the organizational structure and roles granted to them.

4. How will you educate individuals/users having authorized access about the misuse of PII data? Will users receive privacy training before gaining access to the system?

Users sign the Rules of Behavior (ROB) agreement and take annual training on IT Security Awareness training and PII. Users also follow a procedure for requesting access/release of data.

5. Has the data in the system been encrypted according to the National Institute of Standards and Technology (NIST) requirements? (Note: this requirement is for sensitive PII only)

Yes, there is PII being collected in the AutoAudit application. The encryption option will be deployed in the months to come with NHS solution.

6. Do other systems share or have access to information in this system? If yes, who authorized the sharing? If information is being shared, please provide a copy of any agreements that were issued. (*i.e., System Administrators, System Developers, System Managers*)

      No, the AutoAudit application is exclusively for the OIG.

7. Will other agencies, state or local governments, or other external parties (i.e., non-EPA) share or have access to information in this system? If so, what type of agreement was issued? (*i.e., ISA, MOU, etc.) (If any agreements were issued, the Privacy Program needs a copy for its records*).

      No.

8. Will data and/or processes be converted from paper to electronic? If so, what controls are in place to protect the data from unauthorized access or use?

      No.

9. Will data be shared from a system of records (SOR) with another federal agency? If so, has a computer matching agreement been initiated?

      No.

III. <u>Attributes of the Data</u>

1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed. (*Provide an example or explain*)

      The data collected is relevant and necessary to track individual audit and program evaluation. AutoAudit is an application that supports EPA OIG mission and goals.

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

      Access to AutoAudit is restricted to EPA OIG employees. AutoAudit uses Active Directory credentials to authenticate the user to the Lotus Notes Client. The client software, uses the user's Lotus Notes ID credentials to authenticate the user and restrict access. Roles in the AutoAudit application are assigned per user Lotus Notes ID.

3. Has the system undergone a risk analysis to identify harms that may result from technical failures, malevolent third parties or human error? Yes_<u>x</u>__ No___ (**Note: The risk analysis will help identify possible risks to the data in the system.**)

      Yes.

4. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the requested information? Yes_<u>x</u>_ No___ If yes, how is notice given to the individual? (*Privacy policies must clearly explain where the collection or sharing of certain information may be optional and provide users a mechanism to assert any preference to withhold information or prohibit secondary use.*)

      Yes, the AutoAudit Rules of Behavior (ROB) are given to the new user to read and sign the security awareness form before access is granted. Each user has an opportunity to accept or decline the set of rules. If the user declines, the user does not get access to the AutoAudit application.

5. Where is the on-line privacy policy posted?

A privacy policy warning note is displayed on the AutoAudit application default splash screen when the application is launched.

IV. Maintenance and Administrative Controls

1. Has a record control schedule been issued for the records in the system or the system itself? If so, provide the schedule number. *(You may check with the record liaison officer (RLO) for your AA-ship or Tammy Boulware, Headquarters Records Officer, to determine if there is a retention schedule for the subject records. All systems **must** have a record control schedule.)*

Yes, the AutoAudit application is covered under EPA Records Management Policy 420 (paper and electronic records).

2. While the data are retained in the system, what are the requirements for determining that the information collected remains sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The managers review the data for accuracy prior to making decisions. The OIG developed a data quality policy which ensures that proper management responsibilities are in place to comply with EPA's Information Quality Guidelines (OMB Section 515). Annually, the Deputy Inspector General of the OIG certify as a part of the OIG Annual Performance Report, that all data reported through OIG information systems meets the EPA data quality standards.

3. Will this system provide the capability to identify, locate, or monitor individuals? If yes, explain.

No

4. Does the system use any persistent tracking technologies?

No

5. Under which System of Records (SOR) notice does the system operate? Provide the name of the system and its SOR number if applicable. All Agency SORs are posted at http://www.epa.gov/privacy/notice/. *(A SOR is any collection of records under the control of the Agency in which the data is retrieved by a personal identifier. The SOR **must** contain the same categories of records and cover the same routine uses as your system.)*

AutoAudit EPA-50