

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.

All entries must be Times New Roman, 12pt, and start on the next line.

If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Tiger Security (TSEC)		System Owner: Brendon Windmeyer	
Preparer: Alexander Stone		Office: Office of Inspector General (OIG)	
Date: 08/06/2026		Phone: 202-815-9867	
Reason for Submittal: Updating TSEC PIA to include extension to AWS ECHS			
New: ☐	Revised: X	Annual Review: X	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X		Rescindment/Decommission: ☐	
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 OIG TIGER Security (TSEC) is the general support system (GSS) for the OIG internal network. The purpose of TSEC and its supporting components is to provide the OIG with a separate and secure enterprise within the EPA network infrastructure located at Research Triangle Park (RTP) in Durham, N.C and within AWS environment hosted within ECHS. These combined networks provide secure operations for OIG applications in support of the OIG user community. The TSEC environment provides OIG users with access to user and group file shares as well as the OIG server environment.

Section 1. 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?

It doesn't collect, but there are no restrictions on what users or groups can copy to the data folders, so it potentially contains PII and SPII. Under the statute of the Inspector General Act of 1978, 5 U.S.C. app.

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?

An updated SSP has been completed for the system. The current system has an ATO which is set to expire June 26, 2027.

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?

Yes, some data will be stored within AWS hosted on FEDRAMP approved environment hosted by ECHS.

Section 2. 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).

It doesn't collect, but there are no restrictions on what users or groups can copy to the data folders, so it potentially contains PII and SPII including names, addresses, DOB, SSN, etc.

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

The information is stored by users and work groups within the OIG environment using resources such as individual user folders and group folders.

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. The TSEC environment does not collect data from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Individuals or workgroups who copy into the individual or group folders are responsible for the accuracy of the data.

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:

The data that is possibly stored on user folders and group folders includes are not limited to the following; Names, DOB, Addresses, SSN, etc.

Mitigation:

Data encryption and logical restrictions on individual user folder access to only individual users. Restrictions on group folders limited to only applicable groups needing access and limit all file share access to OIG personnel only.

Section 3. 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 use of logical access control is enabled on the file share. Only authorized OIG personnel have access to their individual file share. Furthermore, group folders are logically restricted to individuals who have appropriate group permissions assigned to them in AD.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Yes, there are access control policies and procedures in place. See OIG policy 004-OIG Data quality Procedure- "OIG data are entered into a number of management information systems for internal management accountability and decision-making, and for external reporting in compliance with mission-related and other federal laws and regulations. OIG staff are granted "read" and/or "edit" access to these systems based on their respective role in the organization,

their level and scope of responsibility, and business needs.”

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

TSEC has not only file shares but also has OIG application store

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 internal OIG personnel and their contractors have access. Yes, appropriate FAR clauses are in place.

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.

Files could be stored on shared drives within TSEC that are associated with current IG investigations. In which 1016 records schedule would apply based on investigation and information being stored. The information is kept in accordance to their respected 1016 record schedule

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:

Data is not sanitized according to the 1016 record schedule

Mitigation:

Data is encrypted, and access management audits are conducted on an annual basis.

Section 4. 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.

Information contained within TSEC is not shared externally except as required through FOIA requests and criminal investigations.

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

Data is not shared externally except as mentioned above.

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?

Information is only shared as stated above.

4.4 Does the agreement place limitations on re-dissemination?

No specific agreements are in place.

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 outside the agency, so this is not applicable.

Mitigation:

None.

Section 5. 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 as stated in Section 6.1?

The information is tracked using logs that are reviewed to track unauthorized use. The logs are reviewed to ensure information is used for authorized purpose.

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

Annual ISPAT training is mandatory for all OIG personnel and within 3 days of coming onboard.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

Information leakage during an audit.

Mitigation:

Log files are stored on file share with appropriate access. Only OIG employees with specific logical access to view audit files are permitted to conduct audits of the files and system

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The system serves as a repository for OIG users and groups, as well as application stores.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ 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.

The system is designed to only retrieve the specific information OIG users store in user and group folders. The data is being retrieved using user-specified file names. No files are directly linked to individuals.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The user and group folders have logical access controls on them. The folders individual user folders can only be accessed by the individual user who it is assigned to. The group folders are assigned by AD memberships which control who has access to each folder. The file servers are accessible by approved OIG employees and contractors who approved

logical access to the servers.

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:

Information disclosure to unauthorized individuals not authorized to view contents of file or file share

Mitigation:

Files are restricted to individual users or groups using specified AD groups. Data is also encrypted

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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. 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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 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 Freedom of Information Act (FOIA).

Privacy Risk:

Mitigation:

I attest as the Agency Privacy Officer that **Tiger Security (TSEC)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA

