United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT
(Rev. 2/2020)
(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%20Roster.docx

System Name: SAP SACC People Database	**System Owner: Sharlene Matten**
Preparer: Sharlene Matten	**Office: OPS-MSD-PREB**
Date: 09/20/2021	**Phone:** 202-564-0130
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 FIFRA SAP/ TSCA SACC Database of Scientific Experts contains information on prospective, current, and retired members of the FIFRA Scientific Advisory Panel, the FQPA Science Review Board, TSCA Scientific Committee on Chemicals (SACC), ad hoc experts supporting the TSCA SACC or other scientific peer reviews. The FIFRA SAP and TSCA SACC are peer-review committees formed by EPA under the Federal Advisory Committee Act. The database supports the administrative management of the scientific experts who are members of the Chartered committees or who are additional experts to support the Chartered committees. It is similar in function to the Office of Administrator's Science Advisory Board Database.

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?

The FIFRA Scientific Advisory Panel (SAP) is a statutory advisory committee created on November 28, 1975 pursuant to section 25(d) of the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), as amended by Public Laws 94-140, 95-396, 96-539, 98-201, and 100-532. Section 104 of the Food Quality Protection Act of 1996 (Public Law 104-170) establishes a Science Review Board consisting of sixty scientists who shall be available to the Scientific Advisory Panel on an ad hoc basis to assist in reviews conducted by the Panel. The FIFRA SAP provides independent scientific advice to the EPA on health and safety issues related to pesticides.

The Science Advisory Committee on Chemicals (SACC) was established pursuant to the Frank R. Lautenberg Chemical Safety for the 21st Century Act, Pub. L. No. 114-182, 140 Stat. 448 (2016). The SACC provides independent advice and expert consultation, at the request of the EPA Administrator, with respect to the scientific and technical aspects of issues relating to the implementation of the Frank R. Lautenberg Chemical Safety for the 21st Century Act (the Act), which amends the Toxic Substances Control Act.

Both committees are established in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2.

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?

National Hosting System (NHS), 16 Jan 2023

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.

Confidential Financial Disclosure Form for Environmental Protection Agency Special Government Employees (EPA Form 3110-48) OMB Control NO. 2090-0029 Approval Expires 06/30/2021. ONLY Signature page (with signature dates) are used. Dates are used to track annual completion of this form. No financially sensitive information is provided in the FIFRA SAP/TSCA SACC Expert Database. The complete form is not stored in the database.

OGE Form 450, 5 CFR Part 2634, Subpart I U.S. Office of Government Ethics (Jan. 2019). Expires 11/30/21. ONLY Signature page (with signature dates) are used. Dates are used to track annual completion of this form. No financially sensitive information is provided in the FIFRA SAP/TSCA SACC Expert Database. The complete form is not stored in the database.

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, this **is not** a Cloud platform. All data will be stored on premise in the NHS environment.

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).

- First Name or initial
- Last Name
- Middle Name or initial
- Name Comments
- Person title
- Suffix
- Gender
- Home Address
- City
- State or Province
- Country
- Zip Code
- Home Phone
- Professional Title
- Department
- School or Unit
- University or Organization
- Work Address
- Work City
- Work State or Province
- Work Country
- Work Zip Code
- Work Phone
- Fax Work Phone
- Cell Phone
- Email Address
- Courier Address
- Courier Phone Number (add)
- Zip Code
- Appointment Date

- Citizenship (Add)
- Appointment Expiration (NTE)
- SGE or RGE
- Member of Chartered Committee
- Sponsoring DFO
- Dual Appointment (e.g., SAB and FIFRA SAP)
- Advisory Committee Experience
    - Meeting and Date specific information?
- Hours worked
- Ethics Training Date
- Financial Disclosure Form
    - Submitter Date
    - Intermediate Reviewer Date
    - DEO Date
- CV
- BioSketch
- Technical discipline/expertise

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

Data are taken from existing records.

Each person in the Database supplies this information to EPA either in hiring papers submitted prior to employment (if they are not federal government employees) (e.g., name, address, citizenship as noted in 2.1), signatures & dates from Confidential Financial Disclosure Form (EPA Form 3110-48, see response to Question 1.3) or in emails/discussions with FIFRA SAP/SACC Team staff. Hiring/personnel forms ARE NOT stored in the FIFRA SAP/TSCA SACC Experts Database.

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

2.4 Discuss how accuracy of the data is ensured.

The FIFRA SAP/SACC Team staff (system owners) verify the data with each individual prior to entry into the Database and on an approximately annual basis.

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 is risk that data may be accessed by unauthorized users or intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls in place to mitigate associated risks: Access Control (AC)-System access is limited to personnel with a need-to-know and Audit (AU)-system access is recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise/common controls are in place to monitor, detect and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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. EIAM/WAM is responsible for authentication security for applications. The different levels of assess are: Administrator, Contributor, Reader

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

Authentication security is typically handled by SOP's at the application level.

Access controls will be documented in OMS SSP – NHS.

\

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

Yes. Administrator, Contributer, Reader. All members of the Peer Review and Ethics Branch, Mission Support Division, Office of Program Support, Office of Chemical Safety and Pollution Prevention may enter or edit information. No other staff/managers have access to the database.

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 and management within the Peer Review and Ethics Branch, Mission Support Division, Office of Program Support in OCSPP. NOWSEE grantees trained to use the

data/information in the system may also have access. There are no contractors.

Entry into the database is through WAM authentication. Logging in requires the EPA user's Network ID though Single Sign On (SSO) which will pass the unique ID through HTTP Headers to the application.

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.

OCSPP is working with the NRMP to assign the database to the appropriate schedule. An analogous database, SAB People Database, is listed under EPA Records Schedule Number 0090, "Administrative Support Databases." All records are disposable. Follow the disposition instructions for the related records as discussed in EPA Records Schedule Number 0090.

3.6 Privacy Impact Analysis: Related to Retention

No Sensitive PII is maintained or retained within system. Records which can be accessed through public records are considered low risk if exposed.

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. **See below**

Privacy Risk:

The longer records are retained the greater the likelihood data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

Data records are disposed of in accordance with EPA's record schedule 0090 (the NRMP is in the process of adding this database to EPA records schedule 0090) retention requirements. The system security plan outlines additional system level security controls in place to further mitigate risk: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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?

N/A

Privacy Risk:

None. There is no external sharing.

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 as stated in Section 6.1?

The team in OCSPP/OPS/MSD/PREB is trained to ensure the data are used for the appropriate purpose. By design and application, the database is used as an administrative database to help the Designated Federal Officials and Administrative Team who support the FIFRA SAP and TSCA SACC. The database gathers information/data from other records systems in one place to increase the efficiency of work by those who support the FIFRA SAP and TSCA SACC in the Peer Review and Ethics Branch, Management Support Division, Office of Program Support, Office of Chemical Safety and Pollution Prevention. By design the Application and Database only captures data elements relevant to the purpose of the Application itself. Therefore, it is implicit that the systems design ensures that only relevant information can be entered and/or retained.

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

All EPA staff are required to take annual mandatory information security and privacy awareness training and adhere to other standard Agency training requirements. System users do not receive privacy training specific to SAP.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability.

Privacy Risk:

Lack of or failure of auditing and accountability controls increases the likelihood that data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls are in place: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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.

This information is being collected so that FIFRA SAP/SACC staff can identify available and qualified experts to perform reviews on scientific issues related to pesticide and other chemical uses.

SAP/SACC staff need to be able to quickly search this database and contact perspective review participants.

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.)

Information is retrieved by disciplinary expertise, e.g., developmental toxicology, ecotoxicology, environmental fate, new approach methodologies, risk assessment or hiring date or "not to exceed" date for a personnel action or ethics training date. In doing so, a group of individuals is identified.

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?

Annually, system personnel: review the Privacy Impact Assessment, perform a risk assessment, and undergo an independent security assessment that evaluates system security controls including privacy controls. The system only presents data that is already made available by the Agency. The data is used to develop a risk profile for the Agency based upon the SAP application data elements.

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 is risk associated with the unauthorized use of information.

Mitigation:

An Annual security assessment is conducted to determine the efficacy of implemented security controls. Additionally, the SAP application regularly performs continuous monitoring activities to include configuration management settings audit and vulnerability scanning. A plan of actions and milestones (POA&Ms) is maintained to manage findings identified during these and other continuous monitoring activities.

***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 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: