EPA 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: Science Advisory Board (SAB) Application** | |
| **Preparer: Aaron Yeow/Khanna Johnston** | **Office: AO/Science Advisory Board Staff Office (SABSO)** |
| **Date: 6/11/2020** | **Phone: 202-564-2050/202-564-2820** |
| **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 ☐<br>**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).**<br>**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:

This is revised PIA for and existing system that is being migrated from Lotus Notes to Oracle.

The data collected is used to 1) contact experts regarding advisory committee activities; 2) meet requirements under the Federal Advisory Committee Act to inform the public about experts serving on committees through hard-copy rosters of committees and panels. This information is shared through Web posting of rosters; and 3) finally, when a potential project is upcoming staff may use the database to evaluate prospective experts for possible service on advisory committees and panels.

The database is used to collect professional contact information (such as professional title, institutional affiliation, and work contact information) from individuals who are willing to serve on a committee or panel; terms of appointment to advisory committees and panels; expertise information (such as curricula vitae, professional biosketches; and tracking of administrative information (tracking of filing SGE paperwork, tracking of completion of required training, and tracking of submission of required forms).

## 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 Science Advisory Board Staff Office assists EPA with providing management and technical support to two scientific and technical advisory committees (the Science Advisory Board and the Clean Air Scientific Advisory Committee). Both the SAB and CASAC are Statutory committees created to meet requirements under the Environmental Research, Development, and Demonstration Authorization Act (ERDDAA) (42 U.S. Code § 4365) resulting in the establishment of SAB and the Clean Air Act (CAA) (42 U.S.C. § 7409(d)(2)) resulting in the establishment of CASAC.

Both committees are Federal Advisory Committees and must comply with the Federal Advisory Committee Act (FACA) (5 U.S.C, App.) and related regulations. The agency uses these committees to:

- review the quality and relevance of the scientific and technical information being used by the EPA or proposed as the basis for Agency regulations;
- review EPA research programs and plans;
- provide science advice as requested by the EPA Administrator, and
- advise the agency on broad scientific matters.

In order to increase public comment and improve transparency, the SAB Staff Office requests nominations of experts from the public wishing to nominate themselves or others for committees and panels providing advice; identifies experts to become Special Government Employees (SGEs) serving on advisory committees and panels; ensures that SGEs comply with ethics training and financial disclosure requirements of the Ethics in Government Act (forms are not housed in the database); and coordinates experts' participation in advisory projects and public meetings. The SAB Staff Office conducts these activities to provide the EPA Administrator with scientific advice from balanced committees of qualified experts on high priority science issues. The SAB Database of Scientific and Technical Experts assists the SAB Staff Office to achieve this goal in an efficient manner that protects the privacy of scientific experts.

### 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?

The system will be reside in the Oracle environment at the EPA National Computing Center (NCC) National Hosting Service (NHS). Oracle is considered to be a minor application to the NHS General Support System (GSS) and is a system component of the NHS Application Environments, configured according to the NCC Configuration SOP and therefore OMS does not have an ATO for Oracle. The SAB application has a FIPS 199 Low Categorization and has been issued a security certificate.

### 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, the system will not be stored on the Cloud. It is being migrated from Lotus Notes to Oracle**.**

## 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 collects names, professional affiliations, professional addresses, professional phone numbers, professional email addresses, curriculum vitae, and biosketches (1-2 paragraph biographical summary of nominee qualifications).

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

The Agency solicits nominations of Committee members in the Federal Register Notice. As part of the nomination process, names, affiliations, cvs, biosketches of nominees are submitted by public nominators, EPA staff, and the nominees themselves (self-nominations) through the EPA SAB website or sent directly to the EPA SABSO Staff.

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

The system does not use information from commercial sources. The system collects data from EPA staff, and what nominees themselves submit. Some of this information is already publicly available (names, affiliations, professional contact information, biographical sketches, cvs).

### 2.4 Discuss how accuracy of the data is ensured.

All nominees are contacted and asked if they are interested in being considered for the committees and if so, to provide their biosketches and cvs. By obtaining the information directly from the nominees themselves, accuracy of the data is ensured.

### 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 a risk of inaccurate information about nominees provided by nominators.

**Mitigation:**

Nominees are contacted about their nominations and if interested in being considered, provide their information themselves. This ensures the accuracy of information.

## 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. There is an Access Control List (ACL); and the ACL explains who may access the system, and lists authorized users assigned a specific role. Users may not be able to see the entire system. The SABSO database administrator grants permission and removes permission to certain folders or roles. All users cannot see each portion. Different portions of the system are only accessible based on different user roles. This is to ensure and protect the privacy of the scientific experts the agency uses.

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

The access control levels will be documented in a User's Guide and/or Standing Operating Procedures for the application.

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

Yes. There is an Access Control List (ACL); and the ACL explains who may access the system, and lists authorized users assigned a specific role. Users may not be able to see the entire system. The SABSO database administrator grants permission and removes permission to certain folders or roles. All users cannot see each portion. Different portions of the system are only accessible based on different user roles. This is to ensure and protect the privacy of the scientific experts the agency uses.

### 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 EPA SABSO staff and EPA database support contractors are the only ones who have access to the Database. The appropriate Federal Acquisition Regulation (FAR) clauses are included in the contract.

### 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.

EPA Records Schedule 1024 governs Federal Advisory Committee Records. The records in the database pertain to Item a – substantive committee records related to committee membership. Records under Schedule 1024 are permanent.

### 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:**

**A risk of human error could lead to the accidental deletion.** EPA Records Schedule 1024 governs Federal Advisory Committee Records and are permanent.

**Mitigation:**

The agency always backs up the database in case human error leads to the accidental deletion. Only EPA SABSO personnel and EPA database support contractors have access to consolidated information in the password-protected SAB database. The site is managed by a SABSO database administrator and SABSO supervisor who agree the individual should have access. Persons having authorized access take annual IT Security Awareness Training. There is an Access Control List (ACL); and the ACL explains who may access the system, and lists authorized users assigned a specific role. Users may not be able to see the entire system. The database administrator grants permission and removes permission to certain folders or roles. The agency always backs up the database in case human error leads to the accidental deletion of a biosketch or resume. This would be built into the new database as well and a formal schedule would be established.

## 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 by other entities.

### 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?*

**Privacy Risk:**

None, information is not share 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 as stated in Section 6.1?

Only staff managing committees soliciting nominations receive the nominations and only use the information in evaluating nominations for those committees.

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

Individuals (citizens) nominate and enter their own information via a form located on the internet. Persons having authorized access take annual Information Security and Privacy Awareness Training. However, staff does not enter information on the individual. Rather, they may add a date of when the member started working on a project or a date when the annual ethics training was completed.

### 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

**Privacy Risk:**

There is a risk of unauthorized disclosure, unauthorized use, and inappropriate uses of PII related to auditing and accountability.

**Mitigation:**

The SAB information system is hosted within the NHS information system which uses Splunk to audit activity within the environment. Additionally, Splunk logs are sent to the CSIRC information system who manages the Security Incident and Event Management (SIEM) tool ArcSight which normalizes audit events and reports on any detected unusual or inappropriate activity to include but not be limited to the following:

- Unauthorized disclosure of PII
- Unauthorized uses of PII
- Inappropriate uses of PII

## 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.

When the agency is seeking new experts to review a specific project, a call for nominations is done through a federal register notice. The Federal Register Notice (FRN) lists what may be collected and used to 1) evaluate the nominees qualifications 2) contact experts regarding information provided and advisory activities; 3) meet requirements under the Federal Advisory Committee Act to inform the public about experts serving on committees through hard-copy rosters of committees and panels and Web posting of rosters; and 4) evaluate prospective experts for possible service on advisory committees and panels and future committees and panels. A small amount of generally available information such as experts' institutional affiliation and biosketch data is submitted via internet through a form. The system takes this information and populates the database. The FRN includes what may be submitted to be evaluated, and explains the biosketch submitted, if qualifies, will be posted for a short comment period on the public facing website for a 21-day comment period.

Once selected, the information the member shared becomes a repository or library for the SABSO staff. It documents who has served to provide advice and in what capacity. The SABSO staff periodically may comb through the database to see if any expertise may be particularly useful for an upcoming review. If this is the case, the SABSO staff would reach out to the advisory committee member gauge interest and ensure the information in the database is accurate, up to date, and relevant, updating the biosketch as needed.

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

**Example:**
Name
John Doe or Jane Doe

### 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 data in the application is encrypted on the Oracle servers and access to the application is controlled by an Access Control List (ACL), which controls who may access the system, and lists authorized users assigned to specific roles.

### 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 a risk for unauthorized access and use of data elements in the system.

**Mitigation:**

Only SAB Staff Office personnel and a very limited set of database support contractors have access and will use the consolidated information in the password-protected SAB database.

Once the database is built, and converted from Lotus Notes to Oracle, there should be minimal contractor support needed. A small amount of generally available information such as experts' institutional affiliation and biosketch data is already accessible via the public internet.

*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.

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?

Individuals provide data, if the nominee confirms he/she at any time does not want to be included, their name is withdrawn.

### 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:**

There is a low risk that individuals nominated may not be aware that public nominators submitted their information and/or how that information will be used.

**Mitigation:**

Individuals are informed that they were nominated and provided a link to the Federal Register that describes what information is collected for nominations and how it is used. They are then asked if they are interested, and if so, to provide their cvs and biosketches.

## 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?

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 FOIA.*

**Privacy Risk:**

None; there are proper procedures in place for redress.

**Mitigation:**

None.