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: Significant New Alternatives Policy (SNAP) GuideMe (ADC 3434 and 3661)	
Preparer: Margaret Sheppard	**Office: (OAR) Office of Atmospheric Programs, Stratospheric Protection Division**
Date: 09/30/2021	**Phone: 202-343-9163**
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:

SNAP GuideMe is an application that stores and organizes correspondence and policy documents for EPA's Significant New Alternatives Policy (SNAP) Program and related programs. The system was deployed in 2017 through ADC 3434.

The SNAP program is in the process of enhancing the current system by building a ticketing system, entitled the Stratospheric Protection Division (SPD) Questions Response Hub to handle questions and comments from the public through ADC 3661.

The U.S. Environmental Protection Agency's (EPA) Significant New Alternatives Policy (SNAP) program implements section 612 of the amended Clean Air Act of 1990, which requires EPA to evaluate substitutes for the ozone-depleting substances to reduce overall risk to human health and the environment. Under

section 612, manufactures of substitutes for ozone-depleting substances must send information to EPA on health and environmental impacts of the substitutes before introducing them into interstate commerce. EPA reviews such information and issues listings of substitutes for ozone-depleting substances.

The SPD Questions Response Hub will collect questions and comments from the public regarding SPD topics. This system will formalize handling questions and responses received from the public via email and public form submissions. No specific legal authorities or executive orders permit public comments.

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 Clean Air Act is the statute authorizing and defining EPA's regulations, and thus defining the content of the information in the system. The USC citation for the authority for EPA's regulations is: 42 U.S.C. 7414, 7601, 7671 - 7671q**.** Under CAA Title VI and the *Montreal Protocol on Substances that Deplete the Ozone Layer*, SPD protects the stratospheric ozone layer, public health, and the environment by phasing out ozone-depleting substances and smoothing the transition to safer alternatives. Title VI also contains provisions for regulating emissions of ozone-depleting substances, refrigerant management, servicing of motor vehicle air conditioning systems, banning certain products containing ozone-depleting substances that are nonessential uses of those substances, and requiring labels for products containing or manufactured with ozone-depleting substances.

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 application was initially deployed in 2017, and we were able to receive ATO operating under SNAP's application security certificate (ASC). The ASC expires September 28th of 2020. We are submitting another ADC now because we are incorporating additional functionality. For this ADC, we are seeking an "On-Premise Lite ATO".

The ASC was an alternative (to an SSP) for ensuring application compliance with security standards. Security certificates were phased-out earlier this year and were used primarily for applications that had a security categorization of low (under FIPS 199 categorization) and complied with EPA standard configurations. On-Premise Lite ATOs are EPA's replacement for ASC for non-cloud-based applications.

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?

The system is running on EPA's Oracle Fusion Middleware (OFM) environment on physical, non-cloud-based, servers at the National Computing Center (NCC) in North Carolina.

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 existing SNAP GuideMe system makes correspondence and policy documents related to SNAP and other SPD programs accessible in a central location.

The Questions Response Hub will accept the following data fields submitted by persons outside of EPA with questions regarding SPD matters:

Questioner Name,
Questioner Email,
Questioner Phone Number (optional),
Questioner Company (optional),
Question. (The information, decision, or interpretation the questioner is requesting from SPD)

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

Public users will voluntarily submit questions or comments through existing web contact forms to the Questions Response Hub system.

Correspondence and policy documents stored in the core SNAP GuideMe application is provided by EPA.

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 GuideMe application stores correspondence and policy documents (and not traditional quantitative data), and no information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

Questions submitted through the web form are directly entered into the Oracle database without manipulation. Validation on the submitted data will ensure that the required fields (i.e., Questioner name, email and the question) are populated.

The questioner will receive a message confirming the submission based on the server response.

2.5 <u>Privacy Impact Analysis</u>: 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 application will collect two data fields that contain personally identifiable information: questioner name and email. Because questioners request a response, it is necessary to collect these personally identifiable fields. There are 2 primary privacy risks:

1) Information provided by responders could be inaccurate
2) Information could be overly provided.

Mitigation:

We're taking several precautions to ensure that personally identifiable information is protected and used properly:

a) We're limiting the number of staff who can access personally identifiable information to pre-approved EPA staff.

b) All staff accessing the system will be required to submit proof that they completed EPA and contractor annual Information Security and Privacy Awareness trainings

c) Information is not being shared outside of this system, nor will it be linked to other EPA datasets.

d) All personally identifiable information will be securely stored via the internally accessible application. The application is not accessible to external users.

e) The application is hosted on NCC's Oracle APEX server, and the tool inherits all of the server's security protocols.

f) NCC conducts regular audits of logs and can provide system audit and security logs in the event of an incident.

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, access control levels are in place using the NCC's architecture EPA's Web Access Management (WAM)The following points describe the access controls in place.

1) The Question Response Hub is only accessible to internal EPA users. No public portal exists.

2) Only authorized users with a pre-approved LAN account with an EPA user ID will be able to login and view the data submitted via the Questions Response Hub. The application owners or application developers (contractor) add EPA staff that the owners approve and adds to the list of authorized users who may view the data using EPA's WAM system. The application owners manage authorization of users through Web Application Access (WAA) / Community Access / Manage My Groups and Communities from https://waa.epa.gov.

3) Access control levels managed by WAA include:

   a. SNAP_GUIDEME_APPROVED: This is for any staff who is approved to access SNAP GuideME or the SPD Question Response Hub. If assigned as a reviewer or moderator for a question (see 3.3 for additional roles), these users my make comments or answer responses.

   b. SNAP_GUIDEME_ADMIN: This is for any staff who are granted full rights to add or edit information.

   c. SNAP_GUIDEME_STAFF: This access control level is currently not used. This control level would apply to any EPA staff; however, no access rights are provided within the application for these users.

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

Application owners will approve authorized users. Due to the access controls, described in section 3.1, only authorized users with a pre-approved LAN account will be able to login and view the questions submitted via the Question Response Hub. We expect that the number of approved users who will be allowed to view the data will be small (<20 users).

User roles are fully documented in the application's user guide, which is posted within the tool's instructions tab. That user guide can be provided as an attachment (if needed).

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

SPD QRC will have additional sub-roles for EPA staff. These roles are primarily set up to ensure that questions assigned to the appropriate staff and ensure that staff provide responses. All of these roles would require the SNAP_GUIDEME_APPROVED or SNAP_GUIDEME_ADMIN role.

- Main Moderator, which would be the first responder to all questions into the system. This person will be notified of any questions submitted to the SPD QRC. This user can determine if questions require additional review and assign additional staff as appropriate.
- Webarea Contact, similar to the main moderator, would be notified if a question is submitted to the QRC Hub, based on the regulatory topic associated with the submitted question from the web.
- Final Reviewer, for questions that require additional review, this user will be able to approve and submit a final answer to a question.
- EPA Reviewers, who are designated EPA staff that will be responsible for reviewing or commenting on the answer to the question submitted by the questioner.

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?

As described above, only a small group of EPA users can access the guidance and policy documents, the same subset of internal EPA users can access data submitted via the Questions Response Hub. The developing contractor (Abt Associates) also has access to the guidance documents and data submitted via the Questions Response Hub. All of the necessary FAR clauses are included in Abt Associate's 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.

PII submitted via the Questions Response Hub will not be deleted or purged. SPD would like to track the number of questions successfully proceeded each year and would like to be able to reference prior responses. The system does not currently have its own EPA Records Control Schedule. The questions and responses in the system would fall under EPA Records Control Schedule 1023 for Regulatory Development and Implementation.

The application may need to develop a data retention plan to determine how the data are managed if the system is retired.

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 is no risk with respect to data access. There are clearly defined roles and control levels.

The risk is low with respect to data retention. PII submitted via the Questions Response Hub will not be deleted or purged.

Mitigation:

The questions and responses in the system fall under EPA Records Control Schedule 1023 for Regulatory Development and Implementation.

The application may need to develop a tool-specific data retention plan to determine how the data are managed if the system is retired.

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.

The Questions Response Hub will collect questions and comments from the public, which are currently being accepted via contact forms and email. SPD will reply individually to the public submitter with an appropriate response.

Data collected via the Questions Response Hub will not otherwise be shared with any external parties and will not be used for any purpose other than replying to submitters.

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

Data will not be shared externally and will be used solely to reply to public submitters.

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?

The application has no information sharing agreements or MOUs. Given the simplistic nature of the application and proposed system, we do not anticipate a need to share information beyond those who currently have access.

4.4 Does the agreement place limitations on re-dissemination?

There are no current limitations on re-dissemination.

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 isn't shared.

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?

The application contains a field where administrators can verify whether personally identifiable information submitted by users is accurate. If the system gets an undeliverable message when replying to the user, the submitter's email will be noted as inaccurate in the data verification field. Additionally, NCC manages audit logs which are reviewed regularly and can be provided on demand in the event of an incident.

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

All staff accessing the system will be required to submit proof that they completed EPA and contractor annual Information Security and Privacy Awareness trainings.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is low risk associated with an untimely audit

Mitigation:

The SNAP GuideMe team will work with NCC to ensure that regular system audits occur, and that annual Contingency Planning tests are scheduled to retrieve system audit, security, and authentication logs.

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.

The goal of the Question Response Hub is to create a formal system to easily track responses to public questions, both to ensure questions are responded to and to ensure responses are consistent with earlier responses to similar questions. Information submitted via the Question Response Hub will be stored in the Oracle database, and an approved EPA staff member will use that information to reply to the public questioner. The data will also be used to create aggregated statistics of completed questions, and to create a repository of questions, ensure questions are responded to, and that responses can be referenced in the future.

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 primary retrieval of information will be via:

- keyword searches of the submitted question or EPA's response,
- manually or automatically tagged topics, or
- question resolution status (e.g., open/closed).

The system will provide searching capability on name and email, but this is not a primary method of information retrieval.

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

No SORNs apply to the data being collected in the Questions Response Hub.

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:

The main privacy risk is information misuse, either by an authenticated individual or someone who has breached the system.

Mitigation:

NCC manages audit logs which are reviewed regularly and can be provided on demand in the event of an incident. These logs track who has logged-into the system and provide valuable information about potential security breaches.

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

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:

Mitigation: