United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: ENERGY STAR	
Preparer: Alex Darwin/Karen Schneider	**Office: OAR-OAP-CPPD ENERGY STAR**
Date: 9/18/2020	**Phone: 202-343-9752**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ 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 ENERGY STAR program is a voluntary government program that assists businesses and individuals in protecting the environment through superior energy efficiency. ENERGY STAR provides simple, credible, and unbiased information that consumers and businesses rely on to make well-informed decisions to save money and reduce emissions.

ENERGY STAR has several major systems.

1. **The ENERGY STAR Infrastructure** is a non-sensitive and unclassified system that provides computing and hosting services, enabling EPA to fulfill its mission to protect human health and the environment. Information contained on the ENERGY STAR website includes standards, and policies and procedures for providing energy efficient solutions for commercial and personal use. Infrastructure that supports the ENERGY STAR system is provided as a contractor-run system that is operated by General Dynamics Information Technology (GDIT), which is housed in a Commercial Data Center in Northern Virginia. ENERGY STAR is a

General Support System (GSS) hosting of a collection of minor applications for EPA.

ENERGY STAR Portfolio Manager is a no-cost, energy management tool that allows the public to track and assess the energy, water, and waste consumption of their building portfolio. In 2018, it was used by more than 270,000 commercial properties, comprising 26 billion square feet of floorspace, across the nation. The tool calculates a 1–100 ENERGY STAR score, which has become the industry standard for rating a facility's energy performance. Portfolio Manager sits on the ENERGY STAR infrastructure. It is managed separately but it is within the Infrastructure system boundaries.

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?

Clean Air Act Section 103(g). US Code 7403.

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?

Yes, we have a security plan and an ATO. The ATO expires December 21, 2019. The current ATO was extended to allow us to move from hosting at a contractors site into AWS IAAS. We will submit a new PIA with updated information once we are sufficiently moved to the new environment.

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.

Yes.

OMB Control Number: 2060-0528 (Partnership Agreements)

OMB Control Number: 2060-0347 (Portfolio Manager)

OMB Control Number: 2060-0528 (Products)

OMB Control Number: 2060-0586 (Homes)

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?

None of the data is currently stored in the Cloud.

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).

ENERGY STAR Infrastructure contains two systems that contain low sensitive consumer PII:

- **ENERGY STAR Home Advisor** captures first name, email and zip code, and optionally last name and street address. However, we are in the process of removing both last name and street address.
- **My ENERGY STAR** captures first name, last initial, email, and zip code. However, we are in the process of removing both first name and last initial.

These ENERGY STAR systems only contain low-risk business contact information:

- **Portfolio Manager** is a voluntary tool which collects property information (such as business address), operating characteristics (like Gross Floor Area and number of employees), and energy consumption data. This data is used to generate metrics for users to assess the efficiency of their buildings. This information contains business contact information: name, email, organization, job title, and business address. Portfolio Manager information is not disseminated except for buildings who apply for and are awarded ENERGY STAR certification for their property, then the following information is posted on the ENERGY STAR website in our Certified Buildings Registry (https://www.energystar.gov/buildings/reference/find-energy-star-certified-buildings-and-plants/registry-energy-star-certified-buildings):
  - Property Name
  - ENERGY STAR Score/Year of Certification
  - Property Type
  - Gross Floor Area
  - Name of the Company that owns the Building that received ENERGY STAR Certification
- **Qualified Products List (QPX)** collects information about ENERGY STAR certified products. This information is disseminated to the public via the ENERGY STAR website so that the public can find ENERGY STAR certified products. Business contact information is limited to contact names for the partner, the laboratory and the certification body associated with each certified model. This information is only used when EPA has specific questions for certification bodies about the certified model.

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

All information collected is provided voluntarily via a Web form. We collect a person's email address so we can respond, name, subject, and their question. This is low risk PII.

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.

Home Advisor, My ENERGY STAR, and Portfolio Manager are tools for users to improve the efficiency of their homes and buildings. The tools have some data quality controls built in, but we do not do any edits to the data once submitted.

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:

One risk to the characterization of the data is human error which could result in the collection of inaccurate PII.

Mitigation:

As mitigation, we have programmed a "Data Quality Checker" to verify the data.

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. We give access to each system individually and provide limited access on an account level based on roles and privileges.

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

EPA-approved Admin users can access regular user's information based on need (such as if the user is having a problem in their account, this is documented in a user support ticket). The User Support Team and Certification team are the only people who have Admin Access. This access is logged in the system – so you can see what edits the Admin accounts made. Other users cannot access information unless the owner shares the property through Sharing within Portfolio Manager.

These procedures are documented at the application level in concept of operation (ConOps) and system requirements documents located in the ENERGY STAR Confluence repository. The procedures for determining access to ENEGY STAR systems at the enterprise level are documented in the System Security Plan (SSP).

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

No other components are assigned within the system.

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?

Limited EPA staff have access to the data. All our contracts contain the appropriate FAR clauses.

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.

Records where EPA has certified a result or provided official recognition, such as ENERGY STAR Certified buildings or other similar records, are records that have operational value for the program but are not considered essential for the ongoing management of the program and therefore fall under EPA Records Schedule 1035, item c: Routine environmental program and project records. In the ENERGY STAR IT/IM system, users cannot delete this information (because it is saved by the program) and it is kept for *at least* as long as their record retention schedule of ten years.

Other records input by companies should fall under EPA Records Schedule 1035, item e: Other environmental program and project records. These records do not have value once they are superseded, updated, replaced, or no longer needed for the ongoing management of the program or project. This includes information input by users that are not certified by EPA. These files can be destroyed immediately after file closure. File closure, in this instance, includes when a company's information is updated, replaced, deleted by the company, and/or no longer needed for by current agency business. For more information, see here: http://intranet.epa.gov/records/schedule/final/1035.html

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:

Low. There is a risk that some records will be maintained longer than necessary.

Mitigation:

Our record control schedule will be reviewed on an annual basis to ensure they are strictly followed.

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.

Information is shared with Salesforce because they host the database for 15,000 ENERGY STAR Partners. Salesforce is authorized under an ATO led by OCSPP and therefore not

covered in this document, as stated in the introduction of this document. A portion of this Partner information is made public (ENERGY STAR Partner organization names, website, city, state), on the ENERGY STAR website.

ENERGY STAR Portfolio Manager data is not shared outside of EPA as part of normal agency operations, except for the list of ENERGY STAR Certified buildings which is posted on the ENERGY STAR Web site's Building Locator (which posts: building name, address, building owner and property manager).

ENERGY STAR qualified product information is also shared publicly on the ENERGY STAR website.

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

External sharing (with the public via energystar.gov) is the purpose of much of the ENERGY STAR data collection: to give the public information about buying energy efficient products.

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?

ENERGY STAR does not share information with any outside organizations and therefore does not have any MOUs or other special use arrangements with any outside parties as it pertains to ENERGY STAR data.

4.4 Does the agreement place limitations on re-dissemination?

No. ENERGY STAR does not currently maintain any information sharing agreements.

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. We don't share any information with outside parties, so there is no risk.

Mitigation:

None. We don't share any information with outside parties, so there is no risk.

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 information ENERGY STAR collects is used to help the public improve the energy efficiency of their homes and buildings. We have an internal audit system of "integrated

alerts" to ensure that the information is used for this intended purpose.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.
Privileged users receive annual Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

A risk is that users enter incorrect data.

Mitigation:
An audit system of "integrated alerts" is in place to mitigate incorrect data by calling attention to data that is outside of normal bounds.

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.
ENERGY STAR uses the information to provide users specific information to help them improve the energy efficiency of their homes and buildings. ENERGY STAR also uses the information to work with partners to promote ENERGY STAR products, homes or buildings.

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 method is Property ID. The Property ID is linked to the commercial property address.

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

No SORNs apply to these systems

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:
Low. There is a risk that inaccurate data would lead to improper use of data (the ENERGY STAR certification).

Mitigation:

The data is provided directly from the user, there is no middle-man, so there is a higher degree of accuracy.

*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: