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: ENERGY STAR	**System Owner: Alexandra Sullivan**
Preparer: Alexandra Sullivan & Kathryn Duncan	**Office: OAR-OAP-CPPD ENERGY STAR**
Date: 09/30/2021	**Phone: 202-343-9040**
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 ENERGY STAR Program is a voluntary government program that assists businesses and individuals in protecting the environment through superior energy efficiency. The ENERGY STAR Program provides simple, credible, and unbiased information that consumers and businesses rely on to make well-informed decisions to save money and reduce emissions.

The ENERGY STAR system is utilized to support the ENERGY STAR Program and enable EPA to fulfill its mission to protect human health and the environment.

The ENERGY STAR system is comprised of a general support system (GSS) and several major applications:

(1) The ENERGY STAR GSS is a non-sensitive and unclassified system that provides computing and hosting services. The ENERGY STAR GSS hosts a collection of major applications for the ENERGY STAR Program.

(2) ENERGY STAR website includes standards, and policies and procedures for providing energy efficient solutions for commercial and personal use.

(3) My ENERGY STAR and **Home Advisor** are public facing tools designed to help homeowners improve their home's energy efficiency while adding comfort and value. They create a profile of their home's energy efficiency features and get a prioritized list of energy-saving recommendations customized to their home.

(4) ENERGY STAR Portfolio Manager is a no-cost, energy management tool that allows business and organizations to track and assess the energy and water use in their commercial building portfolio. The tool calculates a 1–100 ENERGY STAR score, which has become the industry standard for rating a facility's energy performance.

(5) Qualified Products Exchange (QPX) is a Certified Products submission transaction processing system with a Web Service front-end, feeding into to an authoritative data warehouse and reporting system for ENERGY STAR products. This data is then fed into the Product Finder a series of web-based tools to help consumers easily identify ENERGY STAR products.

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 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, ENERGY STAR is an established system with a a security plan and an ATO. ENERGY STAR is currently transitioning into the EPA AWS IaaS environment and going through the ATO recertification process. As part of this move and recertification, the Security Plan is being updated. The current ATO was extended to 12/21/2020 support the AWS migrations.

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 (ENERGY STAR Partnership Agreements)
OMB Control Number: 2060-0347 (ENERGY STAR Commercial & Industrial Program)
OMB Control Number: 2060-0528 (ENERGY STAR Products Program)
OMB Control Number: 2060-0586 (ENERGY STAR Residential Program)

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. We will be hosted on AWS East which is FedRamp approved. AWS will be providing IaaS service to ENERGY STAR system.

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).

(1) There is no PII data associated with the ENERGY STAR GSS.

(2) ENERGY STAR Infrastructure contains two applications that contain low sensitive consumer PII:

a. **ENERGY STAR Home Advisor and My ENERGY STAR** allows users to create a personal account. Through the account creation, the application captures first name, email and zip code.
b. **ENERGY STAR Website,** through a pledge campaign, captures first name, email and zip code.

(3) These ENERGY STAR applications contain low sensitive PII for commercial and business partners:

a. **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, business 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):

   i. Property Name
   ii. ENERGY STAR Score/Year of Certification
   iii. Property Type
   iv. Gross Floor Area
   v. Name of the Company that owns the Building that received ENERGY STAR Certification

(4) **QPX** collects information about 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. Partners provide their business name, contact name, email, address along with their product specifications they have available.

This information is disseminated to the public via the ENERGY STAR website so that the public can find ENERGY STAR certified products.

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

Home Advisor and My ENERGY STAR: All information collected is voluntary. Public users provide their information when they create an account. This is low sensitive consumer PII.

ENERGY STAR Website: All information collected is voluntary. Public users provide their information when they sign the pledge. This is low sensitive consumer PII.

Portfolio Manager: All information collected is voluntary. Property owners, utilities and other users provide their data through authenticated API and web forms. This is low sensitive consumer PII.

Qualified Products List (QPX): All information collected is voluntary. All information is provided by product manufacturer partners and is submitted through authenticated APIs. This is low sensitive consumer 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.

Yes. The following information is used:

- **Geographic Mapping Data**: (Source: Open Street Maps) ENERGY STAR uses mapping data to pinpoint the location of ENERGY STAR certified properties, utilities, plants and retail product partners.
- **Weather Station Data**: (Source: National Climatic Data Center) Weather station data is used for several metric calculations such as the ENERGY STAR score.
- **Consumer Retail Pricing Data**: (Source: Various Consumer Retail Partners) Consumer retail pricing data is used in the Product Finder Tool to provide consumers with pricing information for ENERGY STAR certified products in their area.

- **Electric Vehicle (EV) and Incentive Data**: (Source: FuelEconomy.gov) EV data is used to provide consumers with electric vehicle information and available incentives for purchasing electric vehicles and plug-in hybrids.
- **Consumer Product Rebate Data**: (Source: Various ENERGY STAR Utility Partners) Rebate data is used to provide consumers with available rebates in their area.
- **Electric Utility Data**: (Source: Power Profiler) Electric utility data is used by ENERGY STAR for emission calculations.

2.4 Discuss how accuracy of the data is ensured.

All PII submitted via Home Advisor, the ENERGY STAR Website, Portfolio Manager and QPX is voluntary. The applications have basic data quality control checks incorporated into the applications, for example to ensure zip code digit/length and valid domain and formatting for emails. The system also incorporates measures to compare records and prevent duplicate entry. Additionally, administrative modules allow authorized internal system users to review, correct, and or approve user/customer submitted data in accordance with established program SOPs and scheduled data quality checks and scripts.

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:

Low risk.

The primary risk to the characterization of the data is human error, which could result in the collection of inaccurate data. The information itself is categorized low risk because only limited PII is collected.

Mitigation:

As mitigation, the system avoids the collection of unnecessary data and does not capture any sensitive information. In addition, the data quality checks implemented in the system mitigate the risk of inaccurate 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. To support management of the content and data within the ENERGY STAR applications, only EPA approved Admin users have access to the data. Access is given to each application individually with limited access on an account level based on roles and privileges.

- The User Support Team and Certification team are the only people who have EPA - Admin Access to: Portfolio Manager and QPX.

- EPA-approved Admin users can access public user's information based on need (such as if the user is having a problem in their account; this type of activity is documented in a user support ticket.) This access is logged in the system to enable an audit trail for edits the Admin accounts made.

- For the Portfolio Manager Application, public users can only access the information that they entered voluntarily or information shared from other users.

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

These procedures are documented at the application level in concept of operation (ConOps) and system requirements documents located in the application specific ENERGY STAR repository:

- ENERGY STAR website repository
- Home Advisor repository
- Portfolio Manager repository
- QPX repository

The procedures for determining Admin level access to the ENEGY STAR applications, are documented in the ENERGY STAR 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 and contractors have access to the data. The contractors that access the ENERGY STAR system are covered by relevant clauses identified in the Agency's cyber security check-list and/or by the Rights in Data clause (FAR 52.227-14).

The ENERGY STAR applications are public-facing. Customers with password protected accounts have access to the information they have entered voluntarily and that other users have shared with them.

Basic information about energy efficient products and buildings is published by EPA on www.energystar.gov.

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 Awards 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 the 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:

The record control schedule will be reviewed on an annual basis to ensure they are 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.

There is no external sharing of the EPA data with other federal, state and local government, or third-party private sector entities.

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

While there is no sharing of data with external agencies or third parties, some of the data collected is publicly available. Information about ENERGY STAR products and ENERGY STAR partners on the website helps to guide customers to energy efficient choices.

The public sharing of information (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?

Not Applicable.

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 as stated in Section 6.1?

The information ENERGY STAR system collects is used to help the public improve the energy efficiency of their homes and buildings. The primary control is access control. Only those EPA staff or contractors who need access to the information are provided with licenses and access to the systems for specific/intended EPA uses. EPA also uses the ENERGY STAR Certification Standard Operating Procedure (SOP), which details how data should be reviewed to assess and award ENERGY STAR Certification for commercial buildings, and a set of web standards maintained within the ENERGY STAR repository to ensure consistency in how information is presented on the website.

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

All privileged users receive annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low. There is a risk that data could be accessed or modified by authorized and non-authorized users.

Mitigation:

Auditing controls are in place to monitor who is accessing and/or modifying the data in the databases. Additionally, access controls are in place to restrict un-authorized access to the data.

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 ENERGY STAR Program uses information collected by the system to provide the public with information about energy efficiency across the marketplace. The primary purpose of the ENERGY STAR program is to provide resources to the public to help people make informed decisions.

To support these program goals, some information is shared publicly on energystar.gov to provide information to the public and consumers about energy efficient products on the marketplace. Public information includes:

- The list of qualified ENERGY STAR products, which is collected via QPX.
- 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). This information is collected via Portfolio Manager
- The list of ENERGY STAR partner organizations participating with the program, including ENERGY STAR award recipients (includes ENERGY STAR Partner organization names, website, city, state).

Information on these lists is business information that is provided to EPA voluntarily by participating organizations.

ENERGY STAR Program also uses the information to work with individual partners to improve their energy efficiency and/or 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.)

No. Information is retrieved from the system using either the Property ID (identifier for a commercial property) or a Product ID (identifier for a product).

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?

Ensuring that access to the internal applications is restricted; no public users can access the internal administrative functions ensures that the information is handled and used accordingly. The entry into the internal applications is via assigned username and password.

Additionally, the majority of information is contact information for businesses (not individuals), and the scope of information has been limited only to that data which is necessary. Limiting the amount of data collected mitigates possible risk to people with information in the system.

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 risk.
Risk of an inappropriate use of data, such as publishing the wrong information on www.energystar.gov.

Mitigation:

The risk is mitigated by the implementation of access controls to limit access to specific users with a legitimate need to access the data for its intended purpose and the annual IT security awareness training help to ensure data is used in accordance with its intended purposes. In addition, the ENERGY STAR Certification Standard Operating Procedure (SOP) details how data should be reviewed to assess and award ENERGY STAR Certification for commercial buildings, which mitigates this risk by ensuring that accurate information is published to the website when this certification is awarded. Finally, system admin users have the capability to review/retrieved audit logs and additionally check for suspicious activity. All users must be identified & authenticated before accessing ENERGY STAR.

***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: