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: RaterPRO	**System Owner: Alexandra Sullivan**
Preparer: Elliot Seibert	**Office: OAR-OAP-CPPD Energy Star Residential Branch**
Date: 10/30/2020	**Phone: 202-343-9643**
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:

RaterPRO will allow users to collect information on homes that are being rated through the ENERGY STAR Certified Homes program. Note that the RaterPRO system is separate from the other "ENERGY STAR" electronic systems, which is why this separate PIA was created. The program requires a third-party inspector, called a Rater, to perform at least two site inspections of each new home during the course of construction to visually verify compliance with a list of ENERGY STAR requirements as well as to perform a number of performance tests. Currently many Raters use the program's paper checklists to document these inspections. RaterPRO is a free, optional digital data collection platform that Raters can use instead of paper checklists. Alternatively, Raters may choose not to use RaterPRO and use

paper checklists or an alternative third-party record keeping system instead.

Note that, because the work takes place during the home construction phase, in most cases these homes are not yet inhabited or even owned by homeowners. In any case, the system does not link to any information whatsoever about homeowners.

Information is collected by Raters for their own records to document their on-site home inspections. Only users within an organization will have access to the information collected by a user in that organization. EPA will have no access to an organization's collected information. The only exception is that EPA's developer contractor may need to access information in response to a user support request, but in that case they would only be accessing the information for diagnostic purposes.

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?

Legal authority is granted by Clean Air Act Section 103(g), establishing the ENERGY STAR program (42 USC Section 7403g), and the Energy Policy Act that directs EPA to implement "a voluntary program to identify and promote energy–efficient products and buildings" and to "preserve the integrity of the ENERGY STAR label." (42 USC Section 6294a)

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?

An Application Security Certification was received for the system in February 2018 and will expire on 2/10/2021. The certificate is signed by Reginald Slade (IMO), Larry Dollison (ISO) and Betsy Shaw (SIO).

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.

The subset of information covered by the PRA is under OMB control number 2060-0586 and the relevant agency control number is 5900-428.

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. Different parts serve as IaaS, Paas, and Saas. We are using IaaS native AWS solutions

for hosting ECS containers, lambdas, API gateway, etc. CouchDB is PaaS that we use, but we deploy it within our aforementioned IaaS. Terraform, Swagger, and Fastlane are SaaS that we are using to deploy infrastructure and API mapping.

AWS is FedRamp certified at the moderate level.

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).

RaterPRO will allow users to collect information on homes that are being rated through the ENERGY STAR Certified Homes program. The program requires a third-party inspector, called a Rater, to perform at least two site inspections of each rated home during the course of construction to visually verify compliance with a list of ENERGY STAR requirements as well as to perform a number of performance tests. Currently, many Raters uses the program's paper checklists to document these inspections. RaterPRO is a free, optional digital data collection platform that Raters can use instead of paper checklists. The data elements collected are:

- Location of rated home (possibly, but not necessarily, including the home's address.) Note that information about the homeowner is not collected nor usually even known by the Rater.
- Optionally, geo-tag location and duration of site inspections. Users are presented with a system dialog upon first use and have the option to disable this feature at that time, or anytime thereafter via the device settings.
- Dates and times of inspections
- Energy performance specifications of the home, such as insulation R-value and furnace efficiency.
- Compliance (Yes/No/NA) with each ENERGY STAR program requirement, such as air-sealing details and quality insulation installation.
- Photo of the front of the rated home and, optionally, of the other three sides (right, left, back).
- Optionally, textual notes and photos attached to notes.

The RaterPRO app includes the first name, last name, and e-mail address of each user (Rater, a.k.a inspector) in their user profile. The names and e-mail addresses are imported from our existing partner database system ("My Energy Star Account" or MESA) and RaterPRO simply uses the information to identify to whom the user account belongs. When user accounts are first registered, an invitation link is sent to the user's listed e-mail address.

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

There are two sources of data/information in RaterPRO. First, RaterPRO receives user's full

names and e-mail addresses from EPA's MESA partner database. This is used to administer user account profiles. Second, RaterPRO's users enter home record information and inspection results into RaterPRO as detailed above.

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.

Accuracy of the data is not directly assessed. It is left up to each user to ensure the accuracy of the information they enter into RaterPRO.

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:

The primary risk to the characterization of the data is human error, which could result in the entry of inaccurate data by the user. The character of the information is low risk. The user's name and e-mail address is the only information that can be used to distinguish an individual. The bulk of the information collected are home inspection records, which, though linked to individual Raters who performed the inspections, are of little value to anyone but the original rating organization.

Mitigation:

As mitigation, the system avoids the collection of unnecessary data and does not capture any sensitive information. In addition, there is a built-in check to verify names and email addresses to mitigate any 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. Each user has a username and password to prevent access by unauthorized users.

When a Rating Company account is created, one "Admin" user account is created, which is the highest level of user permission. Each company must always have at least one Admin user. An Admin user controls which "Rater" users can access that company's records. Admin users can

restrict a Rater user's access at any point, at which time the user would no longer have access to any of the company's records.

Each Admin user also has the ability to optionally share records with their quality assurance supervising organization, known in the industry as their "Provider organization". Once a home record has been shared with a Provider, it will remain accessible to that Provider in perpetuity.

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

When an organization first requests access to RaterPRO, an e-mail invitation is sent to the "primary" Admin user that the organization has identified. That invitation includes a link to a webpage where that Admin user can setup their username and password. Once their account is activated, that Admin user can trigger invitations to additional users at their discretion. Anyone with contact information registered in EPA's existing contact management system called iStar/MESA is eligible for invitation. It is the responsibility of the Admin user(s) to determine who they would like to invite and grant access.

Admin users may edit or rescind a particular user's access at any point by updating the user's permissions.

Each user has a username and password to prevent access by unauthorized users.

Instructions for this process/policy are included at: **https://www.raterpro.net/#!/support-user-guide-desktop.** Access control is documented in the raterpro support user guide desktop.

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

The assigned roles and responsibilities are:

- **Admin**: Admins are responsible for inviting new users, selecting individual user's roles, creating new home rating records, and optionally submitting completed home ratings to the Provider. This user type has access only to the desktop website and is envisioned to be someone working primarily in the office.
- **Rater**: These users are responsible for performing on-site inspections and recording inspection details. This user has access to the mobile tablet application and is envisioned to be someone working primarily in the field.
- **Provider**: These users may only see completed home ratings that have been submitted to them by Admin users. They can view all home rating collected information, but may not edit the data except to add new comments.

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?
Partners who have set up user accounts will have access to records created within their own Rating Company. EPA will have not access to the data/information. EPA's developer contractor, ICF, will have access to the information only for the purpose of system administration and diagnosing user support issues. These contractors are covered by the Rights in Data clause (FAR 52.227-14).

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.

No EPA records are created by this App. There is no applicable schedule. .

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:

Retaining data indefinitely presents a risk of a large amount of data being exposed in a scenario like an unauthorized data breach. This risk was weighed against the irreversible damage that would be caused by data loss in a scenario where an organization's collected information was automatically purged before they had a chance to make a backup copy.

Mitigation:

As detailed throughout this PIA, significant efforts have been taken to secure the system from a technical perspective against unauthorized access and/or data breach. Furthermore, training and documentation will encourage users to create backups and delete home ratings within the RaterPRO system no later than 3 years after they are created, as a general guideline. Even though this won't be strictly enforced by the system, it is expected that training and education will make this a standard practice so that in reality most records are deleted by users within 3 years of creation.

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.

EPA neither accesses the information collected within RaterPRO, nor does it share the information collected within RaterPRO outside of EPA.

A Rater organization may, optionally, choose to share information on specific home ratings with their Provider organization to assist with their Provider's quality assurance procedures. Alternatively, they may choose to keep using existing methods of information sharing which exist completely outside of RaterPRO such as e-mail or online file sharing. To the extent a Rater organization shares information with a Provider, whether through RaterPRO or otherwise, use of that information would be governed by whatever agreements those organizations put in place with each other as well as the overriding requirements of the verification oversite organization, such as RESNET, under whose auspices both the Rater and Provider organizations operate under. EPA has no specific knowledge or control of those agreements.

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

A main purpose of RaterPRO and the data collection are to foster the reality and the perception of a high level of quality assurance in the ENERGY STAR home certification process. When a Rater organization optionally shares inspection reports with home builders, including the rich data collected within RaterPRO, it creates confidence in the certification process.

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?

There is no access to the system by organizations within EPA. The system does not review or approve information sharing agreements, MOUs, or new uses of the information. It is the responsibility of a Rater organization to determine whether they would like to share information with a Provider organization via RaterPRO and, if so, to put in place appropriate agreements with that Provider organizations.

4.4 Does the agreement place limitations on re-dissemination?

No, there is no limitation on re-dissemination and we anticipate the optional reports will be disseminated in some cases. For example, a Rater organization may share a report with a home builder, who may share the report with a home buyer. This would all be acceptable and compatible with EPA's goals for RaterPRO.

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:

EPA neither accesses the information collected within RaterPRO nor does EPA share the information with any other entities.

If a Rater organization decides to share information with a Provider organization via RaterPRO, there is a risk that the Provider organization will misuse or redistribute that information contrary to agreements between the Rater and Provider organizations (of which EPA has no specific knowledge or control). However, this is no different than the risk that exists with information shared between those organizations using methods other than RaterPRO, such as e-mail.

There is a possibility of a Provider copying information from the RaterPRO system and redistributing it

Mitigation:

RaterPRO is designed so that information sharing, by Rater organizations to Provider organizations, is completely optional. This allows Raters to avoid sharing information if they so desire.

Should a Rater organization share a home rating with a Provider, RaterPRO will limit access to that home rating to that Provider's users. In other words, within the RaterPRO system, access is limited only to those organizations to whom a Rater organization grants access.

There is a possibility of a Provider copying information from the RaterPRO system and redistributing it. This risk is mitigated by password protected accounts that limit organizations to access to their own information only. They are free to share their own information as they please, EPA does not own it.

The risk is mitigated by limiting access to the users/owners of the data only.

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 system's security model, as described above, ensures that each user only has access to the information they are authorized to view. This enforces the roles and access described throughout this PIA.

EPA staff and EPA's developer contractor regularly review the practices stated in this PIA to ensure ongoing compliance.

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

Before an organization is granted access to use RaterPRO, a representative must attend a webinar training**: "**Introduction to ENERGY STAR RaterPRO Version 1.0."

The training covers the user agreement and privacy policy and reiterates that use of RaterPRO is completely voluntary. It also educates the user about how to collect

information within RaterPRO, edit collected information, and delete the information if desired. Furthermore, online documentation is available describing the overall use of RaterPRO and many of the specific topics covered in this PIA including information collection, editing, and sharing.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that a glitch or defect in the systems security code theoretically may allow access to unauthorized users, which would undermine the technical safeguards enforcing the procedures outlined in this PIA.

Additionally, there is a risk that EPA or its contractor's staff may inadvertently act out of accordance with the procedures outlines in this PIA.

Mitigation:

RatePRO has undergone quality assurance testing to ensure that the security model is behaving correctly and limiting access to information to only authorized users. Furthermore, automated and manual test suites are regularly performed on each new version of the system to ensure continued operation as expected.

EPA staff and EPA's developer contractor regularly review the practices stated in this PIA to ensure understanding of and ongoing compliance with this PIA's practices.

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 information will not be directly accessed by EPA. Only users in the Rating Company will have access the home records created by that company. The only exception is that EPA's developer contractor may need to access information in response to a user support request, but in that case they would only be accessing the information for diagnostic purposes.

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 system organizes information as home records. Records are retrieved primarily by home location, which can be specified by the user as an address, community and lot number, or manual identifier. This address is not linked or cannot be linked to an individual. No individual PII is used to retrieve information. To narrow a search, users may filter home records with factors like builder company name or record status (active, complete, deleted, etc.).

Each individual home record includes a record editing history linking the record to the Rater(s) who performed inspections on that home. However, records are not retrievable by Rater identity. For example, the system cannot provide a list of homes inspected by Rater X.

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 controls are technical and administrative. Only EPA's system developer contractors (ICF) have security access to the servers, code and databases. Neither EPA staff nor its program-support contractors have technical access to the system or its data. Administratively, EPA has created and follows a policy that neither EPA staff nor its program-support contractors shall request information collected within RaterPRO. Furthermore, EPA's developer contractors are instructed not to provide such information, should it be mistakenly requested.

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:

Risk EPA employees would access data and misuse the information.

Mitigation:

The risk is mitigated by limiting access to the users/owners of the data only. EPA employee have no access to the individual Rater Organization data and therefore cannot misuse it.

***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: