Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	10/02/23
Departmental Element & Site	Department of Energy (DOE) Bonneville Power Administration (BPA) Portland, Oregon
Name of Information System or IT Project	Comfort Ready Homes – Third Party Website Residential services contract/BAE-GSS
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.
New PIA ☐ **Update** X	This is an updated PIA for an existing third party website.

	Name, Title	Contact Information Phone, Email
System Owner	Yvette Gill, Supervisory IT Specialist	503.230.3904 YRGill@BPA.gov
Information Owner	Margaret Lewis	503-230-7552 MLLewis@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Rachel Hull, CGI FOIA/Privacy Act Officer	(503) 230-5241 rlhull@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, IT Specialist	503.230.5397 HCChoi@BPA.gov
Person Completing this Document	Jonathon Belmont, Residential Sector Lead	503.230.3820 jmbelmont@bpa.gov
Purpose of Information System or IT Project	Comfort Ready Homes is a website that displays weatherization training material and provides business contact information of contractors. The purpose is to train contractors to meet BPA's requirements for energy efficiency in alignment with the Northwest Power and Conservation Council's savings targets, the BPA Energy Efficiency action plan and BPA resource program. All three require additional investment in residential energy efficiency measures that this program will help us achieve. The PII collected through the program website includes names, email addresses and business phone numbers if participants opt in to participation. This information is used to communicate updates to BPA's requirements to participating contractors. On behalf of BPA, Evergreen will use this information to provide contact information for qualified vendors to interested consumers (all vendors opt-in), measure the number of visitors to the different pages of our site, and help make our site content more useful. BPA personnel with admininstrative access to the website do not have access to the PII. BPA admins may request access to contact information via reports. In the event that the contract is not re-awarded after five years, BPA will facitiliate the transfer of the PII to another party, and the PIA will be revised. Comfort Ready Home and associated social media sites are considered a Third-Party Websites/applications and are subject to the requirements of M-10-23. A checklist of these additional requirements was completed and is on file with the BPA Privacy Office. The contract with Evergreen includes five social media sites connected to CRH. - Facebook - LinkedIn - X (Twitter) - Instagram	

MODULE I – PRIVACY NEEDS ASSESSMENT

	- YouTube Privacy Notices and links to BPA's Privacy Policy will be added to all accounts.
Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address Note: Vendor and subscriber Business contact information,including business phone, name, email (business card), service territory. Some BPA personnel will be assigned login credentials for access. ☐ Other – Please Specify
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	N/A – the PII is in the system
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

MODULE I – PRIVACY NEEDS ASSESSMENT

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	YES (If "Yes," place an "X" in the box at the top of first page.) *Member of the Public* refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE
4. Is the information about DOE or contractor employees?	YES or NO (If Yes, select with an "X" in the boxes below) ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) Section 7101, et seq. The Bonneville Power Project: *Administrative Authority to Contract*, Title 16 U.S.C. §§ 832a(f), 839f(a) grants BPA authority to procure contracts to advance the agency's mission.
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Consent is derived through personal participation in the website by all visitors. A privacy notice is included on the website.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	The contract contains the necessary privacy act clauses.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The overall privacy risk is LOW

Confidentiality Factors	Low	Moderate	High
Identifiability	X		
Quantity of PII	X		
Data Field Sensitivity	X		
Context of Use	X		
Obligation to Protect Confidentiality	X		
Access to and Location of PII	X		
Overall Privacy Risk	X		

5. SORNs

How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?

If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

The data will not be retrived by identifier in the regular course of business.

6. SORNs

Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?

If "Yes," provide name of SORN and location in the *Federal Register*.

N/A

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	PII is obtained through manual entry by users who visit the site.
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	Yes – Physical forms will be housed with the vendor and the vendor will be required to store and provide upon request.
DATA USE	
11. How will the PII be used?	On behalf of Energy Efficiency, Evergreen will use this information to provide contact information for qualified vendors to interested consumers, measure the number of visitors to the different pages of our site, and to help make our site content more useful. Vendors OPT IN for this. BPA does not track or record information about specific individuals and their visits, except instances where the individual provides personal information by signing up for our newsletter list or completing a web contact form.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	No

MODULE II – PII SYSTEMS & PROJECTS

13. With what other agencies or entities will an individual's information be shared?	No
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Number of active qualified vendors, training module utilization (not PII), general web analytics • The name of the domain from which the user entered our website (for example, "xcompany.com" if using a private Internet access account). • IP Address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the web). • The type of browser and operating system used to access our site. • The date and time of access. • The pages visited. • If the user navigated to the Network website from another website, and the address of that website. • If the user signed up for our newsletter. • If the user completed a query to a utility or field specialist, or if the user completed a generic contact form, we will gather personal information such as name, email address, mailing address, or telephone number. We may also ask the user to voluntarily share information as part of an online survey. We use this information to measure the number of visitors to the different pages of our site, and to help make our site content more useful. We do not track or record information about specific individuals and their visits, except instances where the individual provides personal information by signing up for our newsletter list or completing a web contact form. This information is not shared with anyone beyond the support staff to this home page, except when required by law enforcement investigation. This information is not sold for commercial marketing purposes.

MODULE II – PII SYSTEMS & PROJECTS	
15. What will be the use of these reports?	It will be used for quality assurance and improvements of the website and supporting program. The following information will be provided to participants: "If you choose to provide us with personal information by signing up for our newsletter list or completing a web contact form, we may use that information to respond to your message or to help us obtain the information you have requested. In an effort to respond to your request, information you submit may be viewed by Comfort Ready Home staff, and, depending upon the nature of your request, shared with utility or BPA staff. Our newsletter list is not sold or shared, and contact queries are used for follow-up purposes only. You may decline emails from us at any time or when you manage your subscriptions. We do not sell, swap, or otherwise share personal information with any other third parties except under the following circumstances: • For analysis, we may share personal information in the aggregate or stripped of any identifying information with BPA. • For legal reasons, we will share information if we are required to by law, regulation, legal process or other enforceable governmental actions. Further, we will share information if the need arises to protect the rights, property or safety of BPA, BPA employees, users or the public."
16. Who will have access to these reports?	BPA EE Administrators will have access to some reports from the site. They won't have direct access to the PII on the site, but that access can be requested as needed.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Information is subscription-based. All subscribers will have the ability to update or remove their contact information at any time should they chose.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	SaaS – Webhosted
Records Management	
22. Identify the record(s).	The website will contain marketing materials for contractors, training materials to perform work to BPA standards, and contact information for program participants.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Records covered under GRS 3.1,General Technology Management Records, and GRS 3.2, Information Security Records, do not need to be included on this form. If the data and records in this system are scheduled as permanent, please review GRS 3.1, item 050 for required documentation for permanent records.
24. Records Contact	IGLM@bpa.gov.
ACCESS, SAFEGUARDS & SECURITY	

25. What controls are in place to protect the data from unauthorized access, modification or use?	Vendor will provide the hosting platform and web on a cloud provider (Amazon Web Services, or AWS), at this time. AWS exceeds all applicable security requirements for physical data centers, including ISO 27001:2013 which provide isolated, containerized environments with dedicated memory, CPU, and other server resources. The vendor will include automated malware and andi-virus applications with daily scanning and an incident response process that provides, upon remedy, reporting to BPA including: • What indicators of compromise were detected. • What steps were taken to clean up the site. • What the initial attack vector was (if identified.) • Our expert recommendations towards remediation steps to prevent further compromise. Security-related patches in software on the servers are automatically applied and validated. • We monitor all high-severity packages running on the server (such as PHP, Apache, NGINX, SSH, OpenSSL, Linux Kernel, and many others) for security vulnerabilities and ensure application of proper patches or remediating steps. User Accounts • Comfort Ready Home is a SAAS platform that utilizes its own local authentication. • These local accounts have a password policy that requires users to create passwords that are at least 8 characters long and contain at least 1 uppercase letter, 1 lowercase letter, and 1 number. • Where possible, users are required to use 2-factor authentication. • Event logs, including logon attempts and failures, successful logons and date and time of logon and logoff, and activities performed by administrators are stored in AWS by local applications for audit purposes. • Logins and passwords are not coded into programs or queries. • Logs are audited monthly by administrators. • At minimum, two administrators have full rights to Comfort Ready Home servers storing data. Granting User Access • Administrative system access is granted to Comfort Ready Home program administrators and access is reviewed and adjusted as necessary.

MODULE II – PII SYSTEMS & PROJECTS	
	• Personnel who have administrative system access use other less powerful accounts for performing non-administrative tasks. Terminating User Access • Terminated employees have their accounts disabled upon transfer or termination. • Since there could be delays in reporting changes in user responsibilities, periodic user access reviews are conducted by administrators. • Transferred employee access is reviewed and adjusted as found necessary. • On a quarterly basis, local accounts are manually audited to verify all users currently need access.
26. Who will have access to PII data?	BPA EE Web administrators via reports Service Contract (Evergreen) web administrators
27. How is access to PII data determined?	Access to modify non-sensitive PII contained in the system will be authorized by the BPA Information Owner
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	There are connected information systems.
30. Who is responsible for ensuring the authorized use of personal information?	The Information Owner – Margaret Lewis, PEP Manager
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2024.04.01 09:13:29 -07'00' (Signature)	
Information Owner	(Print Name) MARGARET LEWIS Digitally signed by MARGARET LEWIS Date: 2024.04.01 13:37:15 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.04.01 16:15:07 -07'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.01 09:59:14 -04'00' (Signature)	