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	12/1/2023
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE) / Joint Office of Energy and Transportation
Name of Information System or IT Project	Electric Vehicle Charging Analytics and Reporting Tool (EV-ChART)
Exhibit Project UID	019-000002823
New PIA X **Update**	This PIA documents the use of the AWS platform to host the EV-ChART system. The application runs in the EITS AWS US East/West cloud service.

	Name, Title	Contact Information Phone, Email
System Owner	Rachael Nealer Deputy Director, Joint Office of Energy and Transportation	202-586-3916 rachael.nealer@ee.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42, Department of Energy	202-287-5786 brooke.dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Omobola Oluwehinmi Information System Security Officer (ISSO)	217- 766- 2087 omobola.oluwehinmi@ee.doe.gov
Person Completing this Document	Justin Gredler Technical Point of Contact Kenneth Macfarlane Technical Point of Contact	571-559-3120 justin.gredler@ee.doe.gov 614-635-0071 kenneth.macfarlane@ee.doe.gov
Purpose of Information System or IT Project	The Joint Office of Energy and Transportation maintains the Electric Vehicle Charging Analytics and Reporting Tool (EV-ChART), which provides a centralized hub for submitting electric vehicle (EV) charging infrastructure data directed by the Federal Highway Administration (23 CFR 680.112). EV-ChART will provide a streamlined data submission process and an integrated set of analytic tools, connect to other data sources, and empower data sharing and access across stakeholders, including the public. Public users are organizations that will provide electric vehicle charging infrastructure data into EV-ChART, for example, electric vehicle service providers (EVSPs), utility companies, gas stations etc. Points of Contact for the organizations will provide first/last name and organization email to facilitate communication between the organization and JOET. This application aims to provide a data platform for electric vehicle industry partners including government entities to upload and maintain data regarding charging infrastructure. Usage data will be generated from electric vehicle charging stations and provided to the system to display an aggregate view. Usage data includes, but is not limited to station locations, charging sessions, station uptime, station outages, installation and maintenance costs, station operators. The user data (email, first and last name) will be retrieved by the application where their professional email will be the unique identifier.	

MODULE I – PRIVACY NEEDS ASSESSMENT

	A user's first name, last name, and corporate email will be used for the purpose of authenticating the user's access to the system and for reporting purposes to track who submitted data. Each user will be aligned to an organization in EV-ChART. Each organization adheres to the following data hierarchal structure: 1) Joint Office and Federal Personnel account has full access to all application data. 2) Direct Federal Funding Recipient (DR) has access to self-data and data their sub recipients submit on their behalf. 3) Sub Recipient of a Direct Federal Funding Recipient (SR) has access to self-data only. For a full detailed list of data modules, see https://driveelectric.gov/files/ev-chart-data-guidance.pdf
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 ☒ Other – Please Specify **(First/Last Name and Organization email address)**
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*	PII is contained in this system. (First/Last Name and Organization email address)

MODULE I – PRIVACY NEEDS ASSESSMENT

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.	
If "Yes," what method was used to verify the system did not contain PII? (e.g., system scan)	Not Applicable.

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
4. Is the information about DOE or contractor employees?	YES. Information may include: ☒ 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.

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?**	42 U.S.C. §16538, Department of Energy Organization Act, 42 U.S.C. § 7101 et seq.; The Economy Act of 1932, as amended (31 US Code 1535), Federal Highway Administration (23 CFR 680.112)
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)?**	All usage of this information is required and only for the function of the application.
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?**	Contractors are involved with the design, development, and maintenance of EV-ChART and are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors. Any information that is obtained or viewed shall be on a need-to-know basis. Assigned contractors are required to safeguard all information they obtain in accordance with the provisions of the Privacy Act and requirements of DOE. The contractors shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed EV-ChART as a Moderate-risk system for confidentiality and integrity, and Low-risk for availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. EV-ChART is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • Audit Logs and Tracking • Encryption • Intrusion Detection • Warning banners and privacy notice • Identity and Authorization Management Security controls (see no. 25 below) will be implemented to ensure that access is restricted according to role, mitigate the risk of accidental sharing, and prevent unauthorized use. This process ensures that controls are operating effectively to mitigate the risk of data (including PII) compromise. While EV-ChART contains some PII, the ensuing risk to the privacy of individuals is generally low as the focus of this application is to provide a data platform for electric vehicle industry partners and government entities to upload and maintain data regarding charging infrastructure. This does not require or encourage collection of sensitive PII and is not driven by analysis of PII.
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 application will retrieve user data (first/last name and organization email). User will create an account on behalf of their organization using login.gov (OneID) to authenticate.

MODULE II – PII SYSTEMS & PROJECTS	
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*.**	Administrative exception to the privacy act applies.
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?	Organization email addresses and first and last name of application users will be provided by representatives of Joint Office of Energy and Transportation, and representatives of Direct Recipient entities (state-level departments of transportation).
9. Will the information system derive new or meta data about an individual from the information collected?	Nothing new or aggregate is being generated from the user data specifically. The information is purely identifier.
10. Are the data elements described in detail and documented?	Yes. For a full detailed list of data modules, see https://driveelectric.gov/files/ev-chart-data-guidance.pdf
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	PII will be used for the purpose of: 1) Authenticating the user's access to the system. • Within the application, user identification, once authenticated, will be used to determine the user's level of access to data and application functions. 2) For reporting purposes to track who submitted data. • A user's access to first name and last name information is determined by their access to the data which has the PII data attached. For example, if User A submits data to which User B has access, User B will be able to see that User A has submitted the data and will be able to identify them by first name and last name. 3) A security measure, used by administrators, to verify who has access to the system. • Within each organization, administrators will know the PII of the users within their organization. This is a security measure for the administrators to confirm the users that have access under an organization.
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 meta data about the PII is collected.
13. With what other agencies or entities will an individual's information be shared?	Not Applicable. Individual information will not be shared with any other agency.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	When data is submitted, a user's first name, last name, and when the data was submitted will be logged to create a tracking history. Reports produced are not about individuals, the reports are about when data was submitted and who submitted the data.
15. What will be the use of these reports?	Not Applicable.
16. Who will have access to these reports?	Not Applicable.

MODULE II – PII SYSTEMS & PROJECTS	
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The application will use OneID as the system of record for user authentication. The OneID may be tracking authentication requests and status for its own purposes, but OneID does not share any data back to EV-ChART other than a response of authentication status for authentication requests initiated by EV-ChART
18. What kinds of information are collected as a function of the monitoring of individuals?	Not Applicable; users of the information system cannot be monitored due to information collected.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Not applicable. Any information regarding user activity in the production environment is available in audit logs, to which access is strictly controlled to approved application operational management team and EITS infrastructure operations. Application audit logs are limited to user actions within the application; there is no tracking of user location or similar data.
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.	Users will be able to update their information (Organization email and first/last name). No PII is shared with, or collected from, any other applications.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Not applicable; current application requirements allow for the operation in one AWS region only (us-east-1). Application data is replicated from us-east-1 to us-east-2 and is utilized only in the event of an application failover.
Records Management	
22. Identify the record(s).	The PII stored by the application will be organization email addresses and first and last name of application users. Non PII information stored includes station locations, charging sessions, station uptime, station outages, installation and maintenance costs and station operators.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The records in this system are unscheduled and must be retained until the records schedule is developed. □ Unscheduled
24. Records Contact	Tia Alexander EERE Records Officer Tia.Alexander@Hq.Doe.Gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Audit Logs and Tracking Intrusion Detection Warning banners and privacy notice Encryption of data at rest and in transit Identity and Authorization Management Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Read Only access to specific resources will be provided; this does not allow access to the database. The database will only be accessible to specified access roles generated through the application. A user's first name, last name, and organization email will be used for the purpose of authenticating the user's access to the system and for reporting purposes to track who submitted data. Each user will be aligned to an organization in EV-ChART. Each organization adheres to the following data hierarchal structure: 1) Joint Office and Federal Personnel account has full access to all application data 2) Direct Federal Funding Recipient (DR) has access to self-data and data their sub recipients submit on their behalf 3) Sub Recipient of a Direct Federal Funding Recipient (SR) has access to self-data only
27. How is access to PII data determined?	The application will identify the access context through the combination of scopes provided by the user pool group and organizational relationship. This is to compartmentalize the data being presented to application users. A user belongs to a specific organization and each organization adheres to the following user creation structure: 1. Joint Office and Federal Personnel (JO) – a member from the JO can add users into this organization 2. Direct Federal Funding Recipient (DR) - A user within the DR organization or within the JO organization can create a DR user 3. Sub Recipient of a Direct Federal Funding Recipient (SR) - A user within the SR, DR, or JO organization can create a SR user
28. Do other information systems share data or have access to the data in the system? If yes, explain.	There is no interconnection, and data is not shared with another system.
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?	Not Applicable. There is no interconnection with another system.

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	System Owner in coordination with the Privacy Team.

END OF MODULE II

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Rachael Nealer** (Print Name) (Signature)	
Local Privacy Act Officer	**Brooke Dickson** (Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.12.01 13:06:36 -05'00' (Signature)	
Chief Privacy Officer	**Ken Hunt** (Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2023.12.01 13:06:55 -05'00' (Signature)	