Affects Members Of the Public? □

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY IMPACT ASSESSMENT		
Date	November 3, 2022	
Departmental Element & Site	Office of Environment, Health, Safety and Security Office of Resource Management Office of Information Management	
Name of Information System or IT Project	Employee Concerns Program (ECP)	
Exhibit Project UID	N/A	
New ☒ **Update** □		
	Name, Title	**Contact Information Phone, Email**
System Owner	Helen Heupel, Office of Information Management, Office of Environment, Health, Safety and Security	helen.heupel@hq.doe.gov
Local Privacy Act Officer	Raymond Holmer Director, Office of Information Management	301-903-7325 Raymond.Holmer@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Krystal Harne EHSS Cyber Security Point of Contact EHSS-72	301-903-8283 Krystal.Harne@hq.doe.gov

MODULE I – PRIVACY IMPACT ASSESSMENT

Person Completing this Document	Ricky Marzett II ECP ISSO Contractor to DOE Edgewater Technology Services	240-723-6729 Ricky.Marzett@hq.doe.gov
Purpose of Information System or IT Project	The Employee Concerns Program (ECP) collects information related to the free and open expression of employee concerns related, but not limited, to the environment, safety, health, and management to fulfill the requirements of DOE Order 442.1B. Individuals may submit written concerns to ECP anonymously without including PII. Individuals may voluntarily choose to include PII relating to themselves or their concerns. Administrative PII including business contact information (name, work phone, and email) will be used where provided for communication purposes only. Concerns are processed and reviewed so that a path for resolution may be identified to further employee safety and satisfaction. The system tracks information relating to employee concerns not including PII to track and trend broad, de-identified metrics including number, categories, dispositions, and resolution timelines of employee concerns.	
Type of Information Collected or Maintained by the System:	□ SSN □ Medical & Health Information □ Financial Information □ Clearance Information □ Biometric Information □ Mother's Maiden Name □ DoB, Place of Birth □ Employment Information □ Criminal History ☒ Name, Phone, Address ☒ Other – Individuals may choose to provide PII relating to themselves or their concerns.	

MODULE I – PRIVACY IMPACT ASSESSMENT

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.*	PII exists.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A
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?	NO
4. Is the information about DOE or contractor employees?	☒ Federal Employees ☒ Contractor Employees

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. 7101 *et seq;*
	50 U.S.C. 2401 *et seq.*;
	42 U.S.C. 2201(p);
	42 U.S.C. 7254;
	42 U.S.C. 5801(a).

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)?**	ECP will allow a person to submit an anonymous concern; the submission of PII is voluntary and not required or actively solicited.
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?**	Yes, contractors are involved with the design, development, and maintenance of the system. The contract contains language requiring contractor compliance with DOE regulations and directives. Contractors are also required to sign Non-Disclosure Agreements (NDAs).

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	ECP presents a moderate risk to privacy. Individuals are permitted to submit anonymous concerns containing no PII, which significantly mitigates the privacy impact as well as the risk of privacy harm. All PII is provided by consenting individuals. The system uses non-sensitive administrative PII including business contact information for communication purposes where provided; this non-sensitive PII presents a low privacy impact. Should individuals include sensitive PII, the privacy impact and the risk of harm to individuals could potentially be serious. Should an individual's concerns be exposed it could result in professional harm to that individual as well as personal and social harm which may have compounding effects. ECP observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). ECP does not require or actively solicit PII to further data minimization. The option for anonymous submissions furthers a number of the FIPPs. In addition, use of the PII in ECP is limited to clearly defined business purposes. Access to and use of PII in the system is protected by a series of controls including role and permission-based monitoring controls.
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.**	Data for all applications are stored in a standard relational database and records are selected by attributes such as names/emails and then records are retrieved by a unique number within the database.
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*.**	DOE-3, Employee Concerns Program Records, 74 FR 1000

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?	Individuals. Department of Energy Federal Employees and Contractors.
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, Database Schemas are maintained with relationships and Data Dictionaries for each application.
DATA USE	
11. How will the PII be used?	Business contact information, where provided, is used for administrative (communication) purposes only. Other PII which individuals choose to provide will be used in broad tracking and trending metrics, e.g., categories of complaints. Complaints are processed for identification of a path for resolution.
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?**	N/A

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	None.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports containing administrative PII may be produced for administrative purposes. An Employee Concerns Report (ECP) may have additional PII where volunteered by the complainant.
15. What will be the use of these reports?	Reports containing administrative PII may be produced for communication purposes.
16. Who will have access to these reports?	Only Department of Energy Authorized Federal Employees and Contractors will have access to the reports. Only Administrators and/or Authorized users of the individual system will be able to access the Reports.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	ECP provides no such capabilities beyond what is inherent to business contact information.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Data in ECP is protected by a series of administrative and technical controls which restrict access to authorized individuals for specified and approved business purposes.
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS

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.	The DOE ECP Manager must document an Employee Concern in an ECP case file (hard copy and/or electronic) in sufficient detail to permit processing. The intent of the ECP screening process is to provide a consistent method by which each Employee Concern is reviewed and evaluated, and a path for resolution is identified. The screening must be performed in a time period consistent with the nature and severity of the Employee Concern. An Employee Concern must be tracked until closure. The goal of the ECP is to close Employee Concerns within 90 calendar days from date of receipt of the Employee Concern. However, closure of the Employee Concern will depend on the supporting information and circumstances of the Employee Concern.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system will not be used at more than one site.
RECORDS MANAGEMENT	
22. Identify the record(s).	DOE ECP case files and other relevant records must be maintained in accordance with DOE O 243.1B, Records Management Program, and other applicable laws, regulations, Departmental Directives and direction. GRS 2.3: Employee Relation Records
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N1-434-98-21: Security Emergency Planning and Safety Records
24. Records Contact	Baldev Dhillon, EHSS-70, 301-903-0990, baldev.dhillon@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS

25. What controls are in place to protect the data from unauthorized access, modification or use?	A series of administrative and technical controls are implemented including DOE EITS Moderate Control Baseline and FEDRAMP Moderate Level using Microsoft Azure Cloud. Role-based access controls are in place to prevent unauthorized access or use of data.
26. Who will have access to PII data?	Administrators of the system who are designated by the Federal Program/Project Managers. Users will be provided access as needed to complete assignments.
27. How is access to PII data determined?	Administrators of the system who are designated by the Federal Program/Project Managers. Authorized users are assigned concerns for processing and review.
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?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	Administrators of the system who are designated by the Federal Program/Project Managers. Developers, Network Administrators, System Owners, Third Party Network Support Personnel

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Helen Heupel** **(Print Name)** Helen Heupel Digitally signed by Helen Heupel Date: 2022.11.30 14:25:31 -05'00' **(Signature)**	
Local Privacy Act Officer	**Raymond Holmer** **(Print Name)** RAYMOND HOLMER Digitally signed by RAYMOND HOLMER Date: 2022.11.30 14:33:10 -05'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.11.23 09:26:14 -05'00' **(Signature)**	