Affects Members Of the Public?	Mark if Applicable w/ an 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	12/1/2022	
Departmental Element & Site	Office of Legacy Management, Morgantown, WV	
Name of Information System or IT Project	Requests Tracking	
Exhibit Project UID	Requests Tracking	
New PIA □ **Update** ☒	There is an update to the Records Management section to reflect the new schedule for this system.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Giancarlo Deguia, Records and Information Management Specialist, Archives and Information Management	Office: (304) 413-0809 Giancarlo.Deguia@lm.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Bob Walker, Team Lead, Archives and Information Management	Office: (304) 413-0825 Bob.Walker@lm.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Bob Walker, Team Lead, Archives and Information Management	Office: (304) 413-0825 Bob.Walker@lm.doe.gov
Person Completing this Document	William Travis Software Engineer	Office: (304) 413-0357 99 Research Park Road Morgantown, WV 26505 William.Travis@lm.doe.gov
Purpose of Information System or IT Project	The Requests Tracking Database System is an in-house developed application for the purpose of tracking the number, type, and status of Employees Occupational Illness Compensation Program Act (EEOICPA), Freedom of Information Act (FOIA) and Privacy Act (PA) requests. Both programs are congressionally mandated that require reporting and programmatic accountability of requests through identifiable information requests requiring a search of our records.	
Type of Information Collected or Maintained by the System:	☒ Social Security number 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. fingerprint, retinal scan ☐ Mother’s Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify	

MODULE I – PRIVACY NEEDS 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.*	Yes
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Cyber Security Scan was completed in September 2015; no items were found.

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?	☒ 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?**	• E-Government Act of 2002 • 10 CFR 1004, Freedom of Information, Department of Energy Guidance • 10 CFR 1008, Records Maintained on Individuals (Privacy Act), DOE Guidance • 36 CFR, Chapter 12, Subchapter B, Records Management • DOE Order 243.1, Records Management Program • LM Goal 1 – Protect human health and environmental • U.S. Environmental Protection Agency (EPA) and Federal Regulatory Requirements
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)?**	Wording at the bottom of the request form grants the use of the applicant's information in performing searches. Applicant can choose not to fill out a form for submission.

MODULE II – PII SYSTEMS & PROJECTS

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, LM contractors were involved in the design, and deployment of the Requests Tracking System. Pertinent contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use, and mishandling by assigned personnel.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed the Request Tracking system as a moderate risk system for confidentiality, integrity, and availability. In the cases of EEOICPA requests, the individual's first and last name and SSN are stored in a database. The system utilizes antivirus, firewalls, account permission restrictions, and intrusion detection as measures to protect against breaches in confidentiality. The Request Tracking System 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 • Annual Training The Request Tracking system contains some SPII and the ensuing risk to the privacy of individuals is moderate.
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 user must present appropriate login credentials to access the systems as part of 3-point authentication within the LM Network. PII can be retrieved using the following Identifiers: The requester's name or Social Security number are used in the Requests Tracking application to retrieve requests.

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*.**	Yes, DOE-10. Federal Register / Vol. 74, No. 6 / Friday, January 9, 2009 / Notices, Page 1008
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?	The sources of the information in the system are provided by individuals submitting requests for information (EEOICPA, FOIA, PA, Congressional, Litigation, etc.)
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, the data elements are described in detail and documented in the data dictionary.
DATA USE	
11. How will the PII be used?	The PII will be used to search for records requested for/by the individual. The social security numbers are used to locate the specific information tied to the specific person and/or request. PII is used to search within Content Manager to find relevant documents for the person. Examples of relevant documents located using PII include work and training history, employer/employment information, and medical records (i.e., dosimetry and radiological exposure measurements).

MODULE II – PII SYSTEMS & PROJECTS	
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
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?	None
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
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
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. The System maintains security via 3-Point Authentication. The user must be enrolled in the correct Active Directory (AD) group in order to access the system. AD enrollment is controlled via a file access form (FAF) requiring appropriate supervisor/DOE sponsor approval. Users must also have appropriate permissions within the system to view an individual's information.
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.	Data is not kept current nor is it verified for accuracy. The data is provided at the start of the request process and is only needed and used for the life cycle of this process. Once the request has been closed the information is kept in the database and only accessed for historical needs.
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 is operated at one site. Remote access is provided to the systems from other LM locations. System is in the Record Handling System (RHS) which has additional Cyber monitoring and restricted external access via VPN and Citrix.
Records Management	
22. Identify the record(s).	The Requests Tracking system is scheduled in accordance with applicable NARA and DOE record retention schedules. See system analysis for details.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ Unscheduled X Scheduled (cite NARA authority(ies) below) The system and data will be destroyed when it is no longer needed and in accordance with applicable NARA and DOE record retention schedules. System Schedule: GRS 4.1, Item 010 —Tracking and Control Records, Destroy or delete when 2 years old, or 2 years after date of last entry, whichever is applicable.
24. Records Contact	Kathi Cole
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	System security is maintained by 3-point authentication. All system team members (Federal and contractor) are required to complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing or Annual Cyber Security Refresher Briefing as a prerequisite for access to the system. Administrative controls include non-disclosure agreements and separation of duties, so individuals only have access to the system for specific projects. User accounts are granted permissions within the system based on their role.
26. Who will have access to PII data?	LM & LMS Employees will have access to PII based on their role and with prior DOE Sponsor/Supervisor approval.
27. How is access to PII data determined?	LM & LMS Employees will have access to PII based on their role and with prior DOE Sponsor/Supervisor approval.
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?	No. The Requests Tracking System is not accessible to any other systems.
30. Who is responsible for ensuring the authorized use of personal information?	Data Officer: Giancarlo Deguia
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Giancarlo Deguia** **(Print Name)** Giancarlo S. Deguia Digitally signed by Giancarlo S. Deguia Date: 2023.04.27 09:01:57 -04'00' **(Signature)**	4/27/2023
Local Privacy Act Officer	**Bob Walker** **(Print Name)** ROBERT WALKER 2023.04.27 13:09:18 -04'00' **(Signature)**	4/27/2023
Ken Hunt **Chief Privacy Officer**	**(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.05.01 09:06:58 -04'00' **(Signature)**	