Affects Member 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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	11/9/2022
Departmental Element & Site	Office of Hearings and Appeal DOE Headquarters,
Name of Information System or IT Project	CTMS (Case Management and Mail Log System)
Exhibit Project UID	N/A
New PIA ☐ **Update** X	This is a minor update to the original CTMS PIA, signed 07/02/2021. The update reflects the removal of wording associated with the General Applications Enclave due to the decommissioning of the enclave and change of the System Owner to Matthew Rotman. There have been no changes in the gathering, handling or protection of any Personally Identifiable Information.

	Name, Title	Contact Information Phone, Email
System Owner	Matthew Rotman Supervisory Attorney-Examiner, Hearings and Appeals, HG-4	202-287-1887 Matthew.Rotman@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Acting Director, Privacy Management and	202-287-5786 Brooke.Dickson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT		
	Compliance, IM-42	
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	William Briggs ISSO, IM-63	William.Briggs@hq.doe.gov
Person Completing this Document	Howard Lee Blackard Jr Information Technology Specialist, HG-1	202–287–1159 Lee.Blackard@hq.doe.gov
Purpose of Information System or IT Project	The Department of Energy's (DOE) Office of Hearing and Appeals (HG) is the quasi-judicial arm of the Department of Energy that conducts hearings and issues initial Departmental decisions with respect to any adjudicative proceedings which the Secretary may delegate, except those within the jurisdiction of the Federal Energy Regulatory Commission (FERC). OHA jurisdiction principally includes Personnel Security Hearing Officer functions (10 CFR Part 710) FOIA Requests, Exemption Cases and "whistleblower" complaints filed under the DOE Contractor Employee Protection Program (10 CFR Part 708). DOE HG owns and operates the Case Tracking and Mail Log System (CTMS). CTMS is an administrative application used for recording the receipt of Case documents, staff assignment of a case file, and disposition of case filings; incoming mail and faxes containing information relevant to an individual's personal security clearance, whistleblower information, or information related to FOIA request information. Additional information can be found here: https://www.energy.gov/oha/office-hearings-and-appeals **Case Information:** As a part of the Hearings and Appeals process, members of the public, their attorneys, DOE staff, DOE attorneys, HG judges, and HG attorneys can submit case information by submitting case documents to a shared mailbox, oha.filings@hq.doe.gov, or via fax and mailings. HG administrative case files are logged into the CTMS system from a browser-based data entry form. Once documents are submitted, Only HG staff (Attorneys, Judges, Assistants, and Managers) working on a case can view case files and have access to its contents. CTMS contains information on the following case types: Personnel Security, Freedom of Information Act (FOIA) requests, Whistleblower and Exceptions cases. **Personnel Security:** New Security cases are submitted by DOE security offices to the Office of Hearings and Appeals OHA Filings mailbox to start the process of a new Personnel Security Hearing. Docket staff will created a new case file in CTMS by creating a new case file folder and assigning a Case ID number, Location of security office that submitted the case file, DOE counsel assigned to the case, and the security guidelines addressing the concerns of the individual. Case documents are then uploaded to the CTMS application and stored in the	

MODULE I – PRIVACY NEEDS ASSESSMENT

	secure EITS/AWS hosting environment for the entire life cycle of the case file under Personnel Security and Administrative Review Files. Individuals sometimes include PII information such as SSN, Medical Records and Arrest Records. This information is not stored in our tracking database, as OHA does not track this information. OHA only tracks the disposition of the case file, dates open and closed, case assignments, and processing time within our office. **FOIA Requests:** New FOIA cases are submitted by DOE FOIA office and Individuals from the public to the Office of Hearings and Appeals OHA Filings mailbox to start the process of a new FOIA Appeal. Docket staff will create a new case file in CTMS by creating a new case file folder and assigning a Case ID number, Type of FOIA request, FOIA topics covered, and Assignment to a OHA attorney. Case documents are then uploaded to the CTMS application and stored in the secure EITS/AWS hosting environment for the entire life cycle of the case file under FOIA and Privacy Act – GRS 4.2 item 020, Access and Disclosure Request Files), OHA only tracks the disposition of the case file, dates open and closed, case assignments and processing time within our office. **Whistleblower:** New Whistleblower cases are submitted by DOE Offices and Individuals to the Office of Hearings and Appeals OHA Filings mailbox to start the process of a new Whistleblower case. Docket staff will create a new case file in CTMS by creating a new case file folder and assigning a Case ID number, Location of complaint that submitted the case file, DOE counsel assigned to the case. Case documents are then uploaded to the CTMS application and stored in the secure EITS/AWS hosting environment for the entire life cycle of the case file under Whistleblower – NC1-434-82-1 (old), DOE 6.7 item 120 (new proposed schedule), Hearings and Appeals Case File, and Administrative Review Files. Individuals sometimes include PII information such as SSN, Medical Records and Arrest Records. This information is not stored in our tracking database as OHA does not track this information. OHA only tracks the disposition of the case file, dates open and closed, case assignments and processing time within our office. **Exceptions Case:** New Exception cases are submitted by companies and manufactures to the Office of Hearings and Appeals OHA Filings mailbox to start the process of a new Exception Appeal Case. Docket staff will create a new case file in CTMS by creating a new case file folder and assigning a Case ID number and the case assignment to a OHA attorney for processing. Case documents are then uploaded to the CTMS application and stored in the secure EITS/AWS hosting environment for the entire life cycle of the case file under Exceptions - NC1-434-82-1 (old), DOE 6.7 item 120 (new proposed schedule), Hearings and Appeals Case File, Administrative Review Files. Individuals sometimes include PII information such as trade secrets. This information is not stored in our tracking database as OHA does not track this information. OHA only tracks the

MODULE I – PRIVACY NEEDS ASSESSMENT

	disposition of the case file, dates open and closed, case assignments and processing time within our office. **Case Documents and Files:** Case documents are sent to a shared mailbox oha.filings@hq.doe.gov or via fax and mailings by members of the public or DOE employees. These documents are reviewed by docket staff and uploaded to the CTMS system. Depending on the document type, docket staff will set up a new case file and notify Office of Hearings and Appeals (HG) management for assignment of the case. If the documents are for existing case files in processing, they will be converted from e-mail format or paper format to PDF file format for uploading to the system. When the documents are uploaded, they are time-stamped and tagged for the file type and category with the use of drop-down selections from the CTMS drag and drop utility. Paper is scanned by our docket personnel and is shredded after completion, and the electronic version is then uploaded to CTMS. Under records retention for electronic records, you can scan paper documents and destroy them since the electronic version becomes the original. Case files are assigned a case ID and stored in the CTMS application. Documents are submitted by individuals and their attorneys, DOE attorneys, and HG judges and attorneys. HG administrative case files are logged into the CTMS system from a browser-based data entry form. Users are required to log into this system with 2–factor authentication/PIV. Office managers grant access to the case file. Managers log into CTMS and select the appropriate attorney from a drop-down menu. Managers will grant access to case files to staff attorneys and judges. Case documents are uploaded to the application via a drag and drop component. Information that is uploaded contains official DOE administrative records from DOE staff and Lab sites across the complex. For example, case documents may contain information relevant to an individual's personal security clearance or information related to FOIA request information. Some information is shared on the public energy.gov website under case listings. It is public data depending on what type of case is filed by an individual. Files containing sensitive information can only be retrieved by a FOIA request. A case file could contain several documents, the only information that is posted to the public website is the Decision and Order of the case. Only HG staff have access to CTMS. **Reporting:** All relevant information deemed necessary by HG management is used for reporting via Crystal Reports. Crystal Reports is a reporting application used to create and generate information reports on data collected within the CTMS database. Staff uses reports to report processing time of each case record. CTMS reports consist of information about pending cases, completed cases, and timeliness of staff

MODULE I – PRIVACY NEEDS ASSESSMENT

	processes for reporting to the HG director and managers to gauge the performance of processing. Crystal Reports are not stored in the CTMS system, reports are run by Docket and Managers and are downloaded to the user's workstation for review. **Technology:** CTMS is a Commercial-off-the-Shelf (COTS) application purchased through LegalFiles.com. CTMS is supported with a full system maintenance agreement. CTMS is also supported and monitored by the Office of the Chief Information Officer (OCIO) to ensure the system is in compliance with the National Institute of Standards and Technology (NIST) 800 standards. Continuous monitoring and scanning are applied to CTMS, this system is scanned biweekly for vulnerability and patches.
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
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*	NO

MODULE I – PRIVACY NEEDS ASSESSMENT

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)	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?	YES
4. Is the information about DOE or contractor employees?	YES

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?**	Jurisdiction is conferred on the Office of Hearings and Appeals (OHA) under the following regulations, statute, and delegation order: 1) 10 CFR Part 710 (security clearance eligibility determinations) 2) 10 CFR Part 708 (“whistleblower” adjudications) 3) 10 CFR 1004.1, 1008 (Freedom of Information and Privacy Act Appeals) 4) DOE Organization Act, 42 USC 7194(a) (Applications for Exception) 5) DOE Delegation Order 00-016.00 (Secretarial delegation of authority under DOE Organization Act, 42 USC 7252)
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)?**	In performance its adjudicatory functions, OHA has the authority to obtain information from various parties that file: 1) requests for investigations and/or hearing, 2) appeals of Departmental determinations, and 3) Applications for Exception from DOE regulatory standards. HG is responsible for deciding Applications for Exception from generally applicable requirements of a rule, regulation or order of the Department, and analyzes Petitions for Special Redress seeking "extraordinary relief" apart from or in addition to any other remedy provided in the Department’s enabling statutes. Exception regulations can be found at https://dev.cms.doe.gov/oha/regulations-0. Authority to collect information: 10 CFR Part 710; Freedom of Information/Privacy Act appeals, 10 CFR 1004.1, 1008), 10, CFR Part 708.

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?**	NO
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed CTMS as a moderate risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by NIST. The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. All data in the system is relevant and necessary for OHA to perform the adjudicatory responsibilities delegated by the Secretary of Energy. Privacy Act data must be protected to maintain the integrity of the organization. CTMS is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Encryption on servers that store data • CTMS web portion protects all data in transmission with Secure Sockets Layer (SSL) encryption • PIV card authentication is required for system access • System reviews While CTMS contains PII, the ensuing risk to the privacy of individuals is generally low, as CTMS is an internal only application, and only HG users have access. The focus of CTMS is to serve as an administrative application to record information about case filings, including the initial receipt, staff assignments, and dispositions.

MODULE II – PII SYSTEMS & PROJECTS	
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.**	Depending on the type of case, data may be retrieved by an individual's name, company name, or case ID number.
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*.**	The following Privacy Act SORNs apply to this system: DOE-7, Whistleblower Investigation, Hearings, and Appeals Records, 74 Fed. Reg. 1005 (1/9/2009) DOE-46, Administrative Review Files, 74 Fed. Reg. 1048 (1/9/2009) DOE-55, Freedom of Information and Privacy Act Request for Records, 74 Fed. Reg. 1059 (1/9/2009) DOE-41, Legal Files (Claims, Litigation, Criminal Violations, Patents, and Others).
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The information is principally provided by the individuals themselves and other DOE offices. A DOE contractor/employer of an individual may also provide information in some cases.

MODULE II – PII SYSTEMS & PROJECTS	
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?	Data is documented in the CTMS application. This data includes Case ID, User Assigned, Date Open, Date Closed, DOE counsel, Location, Disposition of cases, Name, and Case type.
DATA USE	
11. How will the PII be used?	All data in the system is relevant and necessary for OHA to perform its adjudicatory responsibilities. CTMS is a Structured Query Language (SQL) database with almost zero PII other than a person's name and case ID. CTMS cannot control what information sent to the system. Individuals submit documents to the case file, documents may or may not contain SSN, DoB, Medical & Health information, Financial Information, Clearance Information, Mother's Maiden Name, Employment Information, Criminal History, Name, Phone, and Address. Information is not tracked in its database. CTMS does not collect or store SSNs; the PII/Sensitive personally Identifiable Information (SPII) selected above was chosen because that data could possibly be uploaded in a case file submission. CTMS web portion protects all data in transmission with Secure Sockets Layer (SSL) encryption. Encryption is also provided on servers that store data. No document containing SPII will be uploaded to the public DOE website. Example case file Decisions and Order documents can be found here: https://www.energy.gov/oha/listings/whistleblower-cases https://www.energy.gov/oha/office-hearings-and-appeals

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?	Decisions and Orders issued by the OHA may contain data regarding the individual. Reports may contain the disposition of a case file and the processing time from start to finish of a case and who was the case assigned to at the time.
15. What will be the use of these reports?	Decisions and Orders are issued by OHA to reach a determination regarding the matter being adjudicated. Managers will review reports to ensure HG is processing case files in a timely manner, also data is used to produce reports about case inventory and dispositions of cases to Management and Secretary inquires. A quick view of this information can be found on our Website at Energy.gov/OHA under annual report.
16. Who will have access to these reports?	OHA managers and supervisors, IT support staff, and individual OHA attorneys with a need-to-know. HG managers determine the need to know based on the case type. Usually any administrative review hearings will be assigned to our staff judges, once a new case is set up in the system a manager will determine the case load of the judges and assign cases accordingly. Reports contain only information about the status of a case file such as open and closed dates, disposition, and assignments along with details about location of office or individual that requested either a hearing or FOIA request.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	NO

MODULE II – PII SYSTEMS & PROJECTS	
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?	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.	The data in the system is mostly provided by members of the public and partially by other DOE offices that are parties to the matter under adjudication. Therefore, data regarding individuals is generally checked by staff for accuracy, relevancy, and completeness at the time it is received and acknowledged. The OHA attorney assigned in each case may also solicit written submissions from the parties and/or conduct interviews to further supplement relevant data placed in the system.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A
Records Management	

MODULE II – PII SYSTEMS & PROJECTS

22. Identify the Record(s)	The system has 2 main types of records, case files and system records. Case File Records: • Personnel Security – ADM 18, 22b (N1-434-03-01, 22b), Administrative Review Files • FOIA and Privacy Act – GRS 4.2 item 020, Access and Disclosure Request Files • Alternative Dispute Resolution – GRS 2.3 item 012, ADR case files – Formal process • Whistleblower – NC1-434-82-1 (old), DOE 6.7 item 120 (new proposed schedule), Hearings and Appeals Case File • Exceptions - NC1-434-82-1 (old), DOE 6.7 item 120 (new proposed schedule), Hearings and Appeals Case File • General - NC1-434-82-1 (old), DOE 6.7 item 120 (new proposed schedule), Hearings and Appeals Case File System Records: • Records relating to system development, management documentation – GRS 3.1 General Technology Management Records • System access records, logs, backups – GRS 3.2 Information Systems Security RecordsSystem records are maintained by OCIO. System is subject to review annually for proper security and documentation.
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)* Personnel Security Files 1.1 Personnel Security Files Disposition Authority Number: DAA-0434-2015-0005-0001 1.2 Administrative Review Files Disposition Authority Number: DAA-0434-2015-0005-0002 1.3 Finding Aids and Indices Disposition Authority Number: DAA-0434-2015-0005-0003 All documents submitted to our OHA filings mailbox are maintained by the DOE e-mail system, all e-mail is maintained for a minimum of 7 years, as stated by the DOE records management office.

MODULE II – PII SYSTEMS & PROJECTS	
24. Records Contact	Maria Levesque, 202-586-9527 Maria.Levesque@hq.doe.gov Janet Fishman, 202-287-1579 Janet.Fishman@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Information is stored in the shared SQL server provided by Amazon Web Service (AWS) hosting; Information queries are run directly from the SQL server when requested by management for detailed reports on HG case files. CTMS is hosted within the AWS/ Energy IT Services (EITS) environment, this application is only available to HG Judges, Attorneys, Docket Staff and Administrator with strict user control and user licensing purchases from the application vendor. Access is controlled by a username and password that is provided by the system administrator, also users cannot access the data without a valid PIV and user end license. Users can only access the case file information they are assigned. If a user needs to access information that they were not initially assigned, the user will need to submit a formal request and receive approval from authorized personnel. Access to the system is further protected by hosting this application within the AWS environment.
26. Who will have access to PII data?	OHA managers and supervisors, IT support staff, and individual OHA attorneys with a need-to-know.
27. How is access to PII data determined?	Only Authorized EITS, AWS and HG staff will have access. Access is restricted by job roles and responsibilities.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	NO

MODULE II – PII SYSTEMS & PROJECTS	
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?	OHA management, OHA cyber security officers, the Legal Files systems manager, and users designated to handle sensitive data.
END OF MODULE II	

SIGNATURE PAGE

System Owner	Matthew Rotman **(Print Name)** Matthew F. Rotman Digitally signed by Matthew F. Rotman Date: 2022.12.14 15:35:52 -05'00' **(Signature)**	_____
Local Privacy Act Officer	Brooke Dickson **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.12.14 16:22:14 -05'00' **(Signature)**	_____
Chief Privacy Officer	Ken Hunt **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2022.12.14 13:58:28 -05'00' **(Signature)**	_____