

PRIVACY IMPACT ASSESSMENT: EERE – Correspondence and Action Tracking System (CATS)
PIA– August 14, 2009



Affects
Members
Of the Public? ☒

Department of Energy
Privacy Impact Assessment (PIA)

See DOE Order 206.1, *Department of Energy Privacy Program*, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	January 14, 2010	
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE) System is located at DOE Headquarters at Forrestal, with all users located also located at Forrestal.	
Name of Information System or IT Project	Correspondence and Action Tracking System (CATS)	
Exhibit Project UID	019-20-01-12-02-3001-00	
New PIA ☒		
Update ☐		
	Name, Title	Contact Information Phone, Email
System Owner	Phil West Director of Technology Advancement & Outreach	(202) 586-2937 Phil.west@ee.doe.gov
Local Privacy Act Officer	N/A	
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Mimi Afework Contract Support Specialist	(202) 586-8970 Mimi.afework@ee.doe.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

	Dennis Bartlett EERE HQ Cyber Security Program Manager	(202) 586-0874 Dennis.Bartlett@ee.doe.gov
Person Completing this Document	Baback Bazri Associate	(703) 377 4172 bazri_baback@bah.com
Purpose of Information System or IT Project	EERE staff members use CATS to assign and track internal controlled correspondence from eDOCS. Users manage the delegation of assignments, correspondence response preparation, and review of completed concurrence packages. The primary mission of the CATS application is to manage and track correspondence assigned to EERE from eDOCS. EERE receives correspondence from Governors, Congressman, Senators, or members of the general public that are submitted to the US Department of Energy and exported from eDOCS into CATS in order to track timely responses by the appropriate subject matter experts.	
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 Correspondence received might contain the name of the author and their company name, if they are writing on behalf of an organization. Additionally, the author's or company's address and phone numbers may also be maintained within the system. ☐ Criminal History	



MODULE I – PRIVACY NEEDS ASSESSMENT

☒ Name, Phone, Address

Correspondence received by the system always contains the name and address of the individual writing the letter and sometimes phone number or email 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 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.

NO

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

The incoming correspondence received, which contains the name, address, company (if applicable), phone number or email address of the individuals who have written the correspondence are scanned in as attachments into the system.

3. Is the information about individual Members of the Public?

YES

The incoming correspondence also comes from members of the general public.



MODULE I – PRIVACY NEEDS ASSESSMENT

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.

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?

44 U.S.C 3501 (Paperwork Reduction Act of 1980)

44 U.S.C. 101 (The E-Government Act of 2002)



MODULE II – PII SYSTEMS & PROJECTS

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 information is voluntarily submitted by the individual or organization corresponding with EERE.
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 maintenance of the system. All contractors are required to sign the HQ LAN Rules of Behavior. Affected contracts include the appropriate FAR privacy contract clauses.
4. IMPACT ANALYSIS: How does this project or information system impact privacy?	The system contains personally identifiable information such as names, phone numbers, addresses and employment information of individuals. This information is low-risk PII and the potential for privacy concerns, if the system happened to be compromised, is low.
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.	Yes, CATS data can be retrieved through a unique identifier, such as: name of the individual.



MODULE II – PII SYSTEMS & PROJECTS

6. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>? If "Yes," provide name of SORN and location in the <i>Federal Register</i>.	No.
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 information is voluntarily provided by employees or members of the public, when corresponding with EERE. All information is acquired through user input.
9. Will the information system derive new or meta data about an individual from the information collected?	No, New or meta data is not derived from the individual's information.
10. Are the data elements described in detail and documented?	CATS does not list and describe the information (i.e. Names, Addresses, Phone Numbers, Email addresses and Employment Information) it collects outside of the database structure.
DATA USE	
11. How will the PII be used?	PII is used by CATS to track responses to the respective employees or members of the public who sent correspondence to EERE.



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, CATS does not derive meta data from an individual's PII.
13. With what other agencies or entities will an individual's information be shared?	CATS does not share information with other agencies or entities.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	CATS does not produce reports pertaining to individuals.
15. What will be the use of these reports?	N/A. CATS does not produce reports pertaining to individuals.
16. Who will have access to these reports?	N/A. CATS does not produce reports pertaining to individuals.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	CATS includes names, phone numbers, addresses and employment information. Therefore, if the system and data is compromised this information could be used to locate individuals
18. What kinds of information are collected as a function of the monitoring of individuals?	Name, Address, email address, phone numbers and employment information are collected but not for the purpose of monitoring individuals.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The CATS system has controls in place to prevent unauthorized monitoring of individuals.
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.	EERE will utilize the records about individuals (i.e. employees and members of the public) to respond to correspondence sent by the respective individual to EERE. The information obtained by CATS is voluntarily provided by the individual; therefore, records are not checked for relevance or accuracy. Additionally, once a response is sent back to the correspondent, it will not be checked for relevance or accuracy. However, the information is generally not used again and is only used to keep track of correspondence activities.
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 along with all users are located at one site, DOE Headquarters – James V. Forrestal Building in Washington, DC. Therefore the consistent use of information is assured.
Retention & Disposition	
22. What are the retention periods of data in the information system?	All CATS information is backed up on a daily and weekly basis. Additionally, quarterly backups are performed with the backup tapes then being rotated off-site on a quarterly basis and archived indefinitely.
23. What are the procedures for disposition of the data at the end of the retention period?	The procedures around records management are documented within DOE Order (O) 243.1, <i>DOE Records Management Program</i>. The EERE Support Team uses BCWipe for sanitization of hard disks on systems that will either be transferred or retired. However, data is retained on backup tapes indefinitely, including PII. Therefore, there is no end to the retention period for CATS data as there is no disposition of data.
ACCESS, SAFEGUARDS & SECURITY	
24. What controls are in place to protect the data from unauthorized access, modification or use?	CATS has controls in place to prevent unauthorized access, modification and use. For a detailed description of logical access controls in place, please reference the CATS SSP dated September 2009.
25. Who will have access to PII data?	CATS System Administrators and individuals assigned to manage the system will have access to PII. Both federal employees and contractors who have access to the system will have access to PII.



MODULE II – PII SYSTEMS & PROJECTS

26. How is access to PII data determined?	The EERE Office of Technology Advancement and Outreach (EE-12) reviews and approves the request. Upon approval, the EERE HQ LAN Administrator creates a Lotus Notes ID and adds the new user to the CATS access control list with specific rights based on the user's role. The EERE HQ LAN support team also installs the Lotus Notes client if the user does not already have the client on their workstation. The Lotus Notes client has to be installed on the user's DOE computer to be able to access the CATS application. EE-12 will request access for a new user that requires administrative functions. The rest of the process is the same as described above for granting access to an administrator. EE-12 employees are system administrators for the CATS application. General CATS users can only access correspondence for the group/program office that they have been assigned to.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes, CATS is also connected with the department's Electronics Document Online Correspondence and Concurrence System (eDOCS). CATS also shares data with the EERE Executive Information System in order to report on performance metrics. This is an internal application under the same authorizing official and the information is not shared outside the organization.
28. 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?	CATS is connected with the department's Electronics Document Online Correspondence and Concurrence System (eDOCS); there is a documented interconnection agreement in place.
29. Who is responsible for ensuring the authorized use of personal information?	System Owner Cyber Security Program Manager

END OF MODULE II