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	April 7, 2022
Departmental Element & Site	Office of Management Office of Administrative Management and Support, MA-42 DOE Headquarters
Name of Information System or IT Project	Courier Packaging Transportation System (CPTS)
Exhibit Project UID	019-60-01-17-02-3021-00
New PIA ☐ **Update** X	June 2019

	Name, Title	Contact Information Phone, Email
System Owner	Drew Campbell Director, Office of Administrative Management and Support, MA-42	202-586-4181 drew.campbell@hq.doe.gov
Local Privacy Act Officer	Ilir Angjeli Office of Corporate Business Operations, MA-1.1	202-586-3282 Ilir.Angjeli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ilir Angjeli Office of Corporate Business Operations, MA-1.1 MA ISSO	202-586-3282 Ilir.Angjeli@hq.doe.gov
Person Completing this Document	Drew Campbell Office of Administrative Management and Support, MA-42	202-586-4181 drew.campbell@hq.doe.gov
Purpose of Information System or IT Project	The Courier Packaging Transportation (CPTS) system uses SCLIntra software to allow DOE Forrestal (FORS) and Germantown (GTN) users in the Office of Administrative Management and Support (MA-42) to track any package and monitor distribution anywhere within the headquarters (HQ) DOE buildings. CPTS supports the Courier Office, Mail Office, and DOE shuttle bus drivers within MA-42 with mail and package distribution and transportation services. In addition, CPTS is used to track the shuttle bus ridership between the FORS and GTN buildings. The Courier Office uses the handheld devices to scan courier packages throughout the delivery process to ensure the package can always be accounted for. The Mail Office tracks registered and special delivery mail with the handheld devices and the bus drivers use the handheld devices to scan and capture the badge information of riders.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Name, Phone, Address (DOE federal or contractor employee name, business phone, routing symbol; name and business address of package recipient outside DOE.) ☐ 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)	

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 or NO (If Yes, select with an "X" in the boxes below) ☒ 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C.), Section 7101 et. seq. Department of Energy Authorization Act, Title 50, United States Code (U.S.C.), Section 2401 et. seq.
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)?**	Information is provided voluntarily.

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?**	Contractors are involved in the design, development, and maintenance of the system. DOE Headquarters Federal and contractor employee information from CPTS may be disclosed to these contractors and their officers and employees in performance of their contracts. Those individuals, provided this type of information, 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 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 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?**	CPTS does not impact privacy or use any technologies that may impact privacy. There is minimal risk to privacy if the system is compromised. The accidental disclosure of the data in the system will not negatively impact individuals since the type of personal information impacted is already publicly available information. CPTS is an intranet-based application and protects data through multiple security controls to mitigate the risk of compromise. The security controls of the system are reviewed annually as part of the Assessment & Authorization process that addresses the National Institute of Science and Technology (NIST) 800-53 Rev.4, Security and Privacy Controls for Information Systems and Organizations controls and ensures the application is compliant with Federal and DOE policies. In addition, CPTS limits access to only DOE authorized users which must authenticate using password-based authentication managed and controlled by the system administrator. Rules of Behavior are signed by the authorized users before gaining access to the system and the consequences for violating DOE rules are displayed and acknowledged at system logon.

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.**	Data is retrieved by the unique control numbers – the tracking number of the package that is linked to the name of the individual.
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*.**	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 data in the system is provided by the individual to whom it pertains.
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?	The data elements are included in the CPTS System Security Plan (SSP).
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	CPTS uses DOE Headquarters Federal and contractor employee information for the purpose of tracking and monitoring the delivery of DOE internal mail and packages and to monitor the rider-ship of the DOE Germantown/Forrestal shuttle bus.
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?**	The system will not use or derive new or meta data.
13. With what other agencies or entities will an individual's information be shared?	No other agencies share data or have access to the data in the system.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are produced on individuals
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?	The system does not provide the capability to identify, locate, or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	The system does not monitor individuals.

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The system does not monitor individuals. CPTS limits access to only DOE authorized users which must authenticate through the use of password-based authentication managed and controlled by the system administrator. Rules of Behavior are signed by the authorized users before gaining access to the system and the consequences for violating DOE rules are displayed and acknowledged at system logon. The security controls of the system are reviewed annually as part of the A&A process that addresses the NIST 800-53 Rev.4, Security and Privacy Controls for Information Systems and Organizations controls and ensures the application is compliant with Federal and DOE policies.
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 provided by the individual to whom it pertains. Therefore, it is determined that the information is accurate, timely and complete at the time it is provided.
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 DOE Headquarters (HQ) only and accessed by authorized users from the DOE HQ The system is hosted at DOE Headquarters by the DOE Office of the Chief Information Officer (OCIO).
Records Management	
22. Identify the record(s).	Courier, package, and bus rider reports.

MODULE II – PII SYSTEMS & PROJECTS	
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) Data in the system is retained for three years in accordance with General Record Schedule (GRS) 10. The messenger service is two years under GRS 12.
24. Records Contact	Drew Campbell
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization (LOW) in accordance with the OCIO Program Cyber Security Plan (PCSP). Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via user-id and password based on user responsibility and job function. These access controls are defined in the CPTS SSP.
26. Who will have access to PII data?	Authorized users on a need-to-know basis have access to CPTS data. Only authorized DOE federal and contractor personnel have access to the data in the system.
27. How is access to PII data determined?	Access to data is determined by evaluation of job responsibilities and organization. The technical controls include restricted access via user-id and password based on user responsibility and job function These access controls are defined in the CPTS Security Plan.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. DOEInfo has a one-way push interface to CPTS in order to provide DOE HQ Federal and contractor employee information for the purpose of tracking and monitoring the delivery of DOE internal mail and packages and to monitor the rider-ship of the DOE Germantown/Forrestal shuttle bus.

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?	There is an Interconnection Security Agreements (ISA) with DOEInfo to ensure the privacy of individuals is protected.
30. Who is responsible for ensuring the authorized use of personal information?	The System Owner and Functional Managers are responsible for assuring proper use of CPTS's information.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Drew Campbell** (Print Name) (Signature)	
Local Privacy Act Officer	**Ilir Angjeli** (Print Name) (Signature)	
Chief Privacy Officer	**Ken Hunt** (Print Name) (Signature)	