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

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	May 2021
Departmental Element & Site	Office of Management DOE Headquarters, Germantown
Name of Information System or IT Project	Sunflower DOE HQ Assets Property Management System.
Exhibit Project UID	019-60-01-17-02-3004-00
New PIA ☐ **Update** x	Sunflower, August 2017

	Name, Title	Contact Information Phone, Email
System Owner	Lisa Peteet Office of Logistics and Facility Operations, MA-43	(202) 287-5496 Lisa.peteet@hq.doe.gov
Local Privacy Act Officer	N/A	
Cyber Security Expert reviewing this	Ilir Angjeli Office of Corporate Business Operations, MA-1.1	(202) 586-3282 Ilir.angjeli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Lisa Peteet Office of Logistics and Facility Operations, MA-43	(202) 287-5496 Lisa.peteet@hq.doe.gov
Purpose of Information System or IT Project	The DOE Sunflower Assets System (Sunflower) is a commercial off-the-shelf (COTS) product acquired to support the DOE property management program. Sunflower is a web-based, centralized database system that permits entry, storage, and reporting of property inventory information. The Accountable Property Representative (APR) in each organization is responsible for maintaining accurate inventory information including current user and location of assets. Sunflower maintains a database that stores information about the assets owned from DOE Headquarters (HQ) and is available for use by DOE HQ Program and Staff offices. In addition, Sunflower records asset information and generates management reports. The acquisition of the assets, control through their life-cycle and the excess of the DOE HQ assets are managed within Sunflower.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number -ENCRYPTED ☐ 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 - Property custodian's name, employee identification, security login, serial number and property tag identification. ☐ 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.*	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?**	NO
4. **Is the information about DOE or contractor employees?**	YES ☒ 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?**	Federal Property and Administrative Services Act of 1949, Section 202(b), 40 USA 483(b) and 41 CFR 109, and Federal Property Management Regulation (FPMR) Subchapter E, part 109.
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)?**	Such opportunities to decline provided information would apply to the DOEInfo system, which is the source for Sunflower information about employees, but does not apply to Sunflower.

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, contractors are involved in the maintenance and customization of the COTS-based system. They do not have access to DOE data as testing with live data is prohibited by DOE policy. Information may be disclosed to contractors and their officers and employees in performance of their contract. Individuals provided this information are subject to the same limitation applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. 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 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?**	N/A
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.**	Records are retrieved by tag number, custodian name, employee identification number, make, model, serial number, security login information, and/or storage location.
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-23, Property Accountability System

MODULE II – PII SYSTEMS & PROJECTS	
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?	Individual user information is provided by DOEInfo or by manual entry by a Sunflower Administrator.
9. Will the information system derive new or meta data about an individual from the information collected?	No, the system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected. The focus is on asset location and control.
10. Are the data elements described in detail and documented?	There is a Sunflower Database Model that describes the data elements in detail.
DATA USE	
11. How will the PII be used?	To provide evidence of assignment, location, and value in the event that government property is lost or stolen.
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	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports are focused on asset control.
15. What will be the use of these reports?	To obtain user and asset information.
16. Who will have access to these reports?	Permission to reports is role-based. The information is available to the System Administrator, Inventory Manager, ACR User, and Query User.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, a user with System Administrator rights in Sunflower would have the capability to identify (but not locate and monitor) individuals, as those individuals are attributes of an asset.
18. What kinds of information are collected as a function of the monitoring of individuals?	None
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.	Sunflower does not verify the accuracy or completeness of the DOE Federal and contractor data in the system. The data in the system is provided by the DOEInfo system. Therefore, at the time the information is provided from DOEInfo, it is determined that the information is accurate, timely, and complete.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Sunflower is a web-based, centralized Oracle database application on the DOE Intranet. As such, there is a consistent interface to the application from within the DOE environment regardless of physical location. Consistent use of this system throughout DOE HQ will be maintained by requiring user training and providing users with system operational documentation.
Records Management	

MODULE II – PII SYSTEMS & PROJECTS

22. Identify the record(s).	Sunflower stores the person's information in the SA_PEOPLE table. It gets automatically updated from the DOEInfo feed on a nightly basis. The process pulls the employee's personal information from DOEInfo and updates the corresponding people records in Sunflower. If person's record does not exist among the records pulled from DOEInfo, it is automatically end-dated in Sunflower (means user is no longer active in Sunflower). If person's record pulled from DOEInfo does not exist in the Sunflower's people table, it gets automatically inserted. The unique identifier currently used to sync the records between the two systems is the "encrypted_ssn" data element. The data attributes updated in the Sunflower's "people" table are listed in the query below: SELECT ""|| ls.encrypted_ssn ||"","|| ls.badge_number ||"","|| ls.employee_name_first ||"","|| ls.employee_name_middle ||"","|| ls.employee_name_last ||"","|| ls.employee_name_suffix ||"","|| ls.record_type ||"","|| ls.personnel_status_code ||"","|| ls.org_1st_tier_code ||"","|| ls.building_code ||"","|| ls.room_number ||"","|| ls.routing_symbol ||"","|| ls.organization_symbol ||"","|| ls.voice_phone_number ||"","|| ls.internet_address ||"","|| to_char(ls.sponsor_date, 'MM/DD/YYYY') ||"","|| ls.guid ||"","|| ls.badge_serial_num ||"" FROM doeinfo.locator_sunflower ls WHERE (ls.badge_number IS NOT NULL AND ls.personnel_status_code IN ('A', '1', '4')) OR (ls.badge_number IS NULL AND ls.personnel_status_code IN ('A', 'N', '1', '4') AND (SUBSTR (ls.duty_station_code, 1, 2) IN ('11', '24', '51')))

MODULE II – PII SYSTEMS & PROJECTS

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	□ Unscheduled X Scheduled *(cite NARA authority(ies) below)* Retention periods are in accordance with National Archives and Records Administration (NARA) and DOE records schedules. Procedures for disposition of data are in accordance with ADMINISTRATIVE RECORDS SCHEDULE 20: ELECTRONIC RECORDS- 1c
24. Records Contact	Lisa Peteet Position: Sunflower System Owner Organization: MA-431 Address: U.S. Department of Energy 1000 Independence Ave., SW Washington, DC 20585 Phone: 202-287-5496 E-mail: lisa.peteet@hq.doe.gov Or Laura Kramer Position: DOEInfo System Owner Organization: CF-40 Address: U.S. Department of Energy 19901 Germantown Rd. Germantown, MD 20874 Phone: 301-903-9932 E-mail: laura.kramer@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?	Sunflower has implemented and all baseline security controls have been tested as appropriate to its FIPS categorization of Moderate in accordance with the DOE HQ PCSP and DOE Directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with system access; by virtue of the role each user is assigned. The technical controls include restricted access via unique user-id and password with access/functional privileges commensurate with the user's job responsibilities. All system team members (Federal and contractor) are required to complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing as a necessary prerequisite for access to the system. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include separation of duties so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system.
26. Who will have access to PII data?	Primary and alternate property custodians and property office staff members.
27. How is access to PII data determined?	Access is authorized only by the System Owner. Administrative controls include separation of duties so individuals only have access to the appropriate personal information.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	DOEInfo has a one-way interface to Sunflower. It scheduled to run automatically via cron job on a nightly basis. The process pulls the employee's personal information from DOEInfo and updates the corresponding people records in Sunflower If a person's record does not exist among the records pulled from DOEInfo, it is automatically end-dated in Sunflower (means user is no longer active in Sunflower). If a person's record pulled from DOEInfo doesn't exist in the Sunflower's "people" table, it gets automatically inserted. The DOE DAYS system shares asset information with Sunflower. It has access to view Sunflower data, which includes assets and an asset's information/attributes (limited to location of asset and the person's name associated with it). The current implementation of the interface is an inbound and outbound feed of information between the two systems. The EERE Data Center (EDC) has a one-way interface with Sunflower. This interface allows the EDC to access, in a read-only mode, the Sunflower database for the purposes of obtaining needed inventory information in support of EDC functionality. The EERE DW 2.0 system has been approved to pull Office of Electricity Delivery & Energy Reliability (OE) data into their system to support the OE Real Property/Inventory Asset Management Team.
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?	Yes, interconnection agreements are in place.
30. Who is responsible for ensuring the authorized use of personal information?	The Sunflower System Owner is ultimately responsible for assuring proper use of the data, but the responsibility extends through the four Sunflower user groups as well.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Lisa Peteet** (Print Name) (Signature)	
Local Privacy Act Officer	**N/A** (Print Name) (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) (Signature)	