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	12/28/2022	
Departmental Element & Site	Office of Legacy Management, Morgantown, WV	
Name of Information System or IT Project	ARCHIBUS	
Exhibit Project UID		
New PIA ☐ **Update** ☒	Please indicate whether this is a new PIA or an update to an existing PIA. List the name of the PIA being updated.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Bud Sokolovich	Bud.sokolovich@lm.doe.gov (303) 410.4810
Local Privacy Act Officer	Bob Walker, Team Lead, Archives and Information Management	Office: (304) 413-0825 Bob.Walker@lm.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Bob Walker, Team Lead, Archives and Information Management	(304) 413-0825 Bob.Walker@lm.doe.gov
Person Completing this Document	Michelle Caldwell Solutions Operations and Maintenance	970.640.2920 Michelle.caldwell@lm.doe.gov
Purpose of Information System or IT Project	ARCHIBUS is a web-based Enterprise Asset Management (EAM) software application that was acquired in 2018, to provide an integrated suite of data functionality and reporting to support LM's Asset Management team. Initially deployed in 2020, the ARCHIBUS system is used for many purposes and serves many key functions. It is Asset Management's source of information for tracking LM's personal property assets, executing yearly inventories, and supports work maintenance activities, including on demand and preventative maintenance work orders for facility management at all occupied sites. Additionally, it captures employee information including assigned seating locations in floorplans and is integrated bi-directionally with building information modeling and computer-aided design (AutoCAD) software. This data allows us to track personnel, performance, and occupancy for space planning and usage. Finally, it provides fleet management functionality including tracking vehicles, dispatch reservations, and fuel transaction information. Future plans for the system are to incorporate condition assessments, reservations and hoteling, lease administration, as well as move management initiatives. Current functionalities and work processes continue to be refined, further developed, and integrated into LM's Asset Management program.	
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. fingerprint, retinal scan ☐ Mother's Maiden Name	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address (name only). The LM Asset Management department uses the system to support and track LM Assets. This is the only use of full Names. ☐ 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.*	Yes
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Visual inspection of data contained in the system.

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?	No
3. Is the information about individual Members of the Public?	No
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.

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?**	What statute, regulation, Executive Order or Departmental authority authorizes the collection and maintenance of personal information to meet an official program mission or goal? As provided in DOE G 580.1-1A, Personal Property Management System—the system of acquiring, maintaining, using and disposing personal property under the stewardship of an organization or entity. Includes monitoring and control functions relative to lifecycle management of the property in support of organizational objectives, sound business practices, and compliance with applicable standards, policies, regulations, and contractual requirements. Archibus is not intended to collect PII. The system is our Personal Property Management System used to associate personal property with a name for lifecycle management.

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)?**	Individuals provide their consent and sign a personal property receipt upon the start of their employment with LM. All personal property is barcoded and assigned to the employee (name only in the system).
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, LMS contractors are involved in the design, deployment, and use of the ARCHIBUS system. Yes, contract flow-down provisions include all applicable privacy related policies, procedures, clauses, statutes, and regulations.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in is limited to clearly defined business purposes. Security controls have been implemented and processes are in place to ensure that access is restricted. Archibus 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 • NDA Agreements The only PII maintained in this system is an individual's name, the ensuing risk to the privacy of individuals is generally low as the focus of is to provide an integrated suite of data functionality and reporting to support LM's Asset Management team. This does not require or encourage collection of sensitive PII. The system also utilizes antivirus, firewalls, account permission restrictions, and intrusion detection measures to protect against breaches in confidentiality. All LM Personnel is required to take annual privacy (PII) training. This ensures that all personnel are trained on the proper use and protection of individual's PII.

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.**	The user must present appropriate login credentials to access the system as part of a multi-point authentication within the LM Domain Network. ARCHIBUS is enterprise-class software operating on a secure platform with external access controls secured through LM network authentication, LM Active Directory and internal controls based on LM user access with custom-configured role-based access.
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?	All personal property is barcoded and assigned to the employee (name only in the system). The information is pulled from our Active Directory which is entered and managed by Asset Management personnel.
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?	N/A
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	Identifies persons on the contract that will utilize personal property and/or fleet vehicles.
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?**	NA
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?	Employee directory and seating/occupancy reports. Data can be sorted in the system to view individual's contact information but no export of this data in a report is available.
15. What will be the use of these reports?	Show active employees, their contact information (work email and phone), status (including remote local vs. remote non-local), department, and an assigned office seating location if assigned (building and room).
16. Who will have access to these reports?	"General Siting" role or read-only users
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?	NA
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Access is limited via operating system access controls lists, network controls and ARCHIBUS application layer role-based security.

MODULE II – PII SYSTEMS & PROJECTS

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.	Regular review of system data against Human Resource department updates.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Access to the system is tightly controlled by the ARCHIBUS system owner/administrator. The data is stored on a central server.
Records Management	
22. Identify the record(s).	ARCHIBUS system is scheduled in accordance with applicable NARA and DOE record retention schedules.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* Records disposition is authorized under Disposition Authority DAA-GRS-2016-0011-0001. General Records Schedule 5.4 Item 010.
24. Records Contact	LMS Information Management
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	System security is maintained by multi-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 necessary 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.
26. Who will have access to PII data?	There is not PII in this system besides the individual's name.

MODULE II – PII SYSTEMS & PROJECTS	
27. How is access to PII data determined?	There is not PII in this system besides the individual's name.
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?	NA
30. Who is responsible for ensuring the authorized use of personal information?	The system owner or designated representative.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Bud Sokolovich** _____ **(Print Name)** _____ **(Signature)**	_____
Local Privacy Act Officer	_**Bob Walker** **(Print Name)** _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.01.16 08:48:50 -05'00' _____ **(Signature)**	_____