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	March 10, 2022	
Departmental Element & Site	Strategic Petroleum Reserve Office – New Orleans, LA 70123	
Name of Information System or IT Project	Physical Security Major Application (PSMA)	
Exhibit Project UID		
New PIA □ **Update** ☒	Updated to utilize the new PIA template, The updated PIA includes the required records review.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Dawn Glapion, Assistant Project Manager, Technical Assurance	(504) 734-4533 Dawn.Glapion@spr.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Kristin Frischhertz, Program Analyst	(504) 734-4297 kristin.frischhertz@spr.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Allen Rome, Cyber Security Program Manager Chris Shipp, Information System Security Manager	(504) 734-4482 Allen.rome@spr.doe.gov (504) 734-4905 Chris.shipp@spr.doe.gov
Person Completing this Document	David Lapuyade, Supervisor ISSO	(504) 734-4605 David.Lapuyade@spr.doe.gov
Purpose of Information System or IT Project	The SPR PSMA manages the physical access control and facility alarm systems at the SPR. The Sitewide Card Access System allows authorized personnel access to SPR facilities using a collection of badge readers and access rules. The SPR does not collect information about members of the general public. All PII information relates to current and former employees and contractors, and only as relates to information needed to conduct business operations.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Other – Vehicle identifiers (e.g., license plates), photographic identifiers (e.g., photographic image)
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 System contains PII.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	PII Risk Assessment was completed.

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 (not the general public, former DOE federal employees and contractors only)
4. Is the information about DOE or contractor employees?	☒ Federal Employees ☒ Contractor Employees

If the answer to **<u>all</u>** 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 I – PRIVACY NEEDS ASSESSMENT

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?**	What statute, regulation, Executive Order or Departmental authority authorizes the collection and maintenance of personal information to meet an official program mission or goal? 42 U.S.C. 7101 et seq., 50 U.S.C. 2401 et seq., 5 U.S.C. 552a (the Privacy Act of 1974), Homeland Security Presidential Directive 12, ''Policy for a Common Identification Standard for Federal Employees Contractors,'' August 27, 2004, and Title 5, Code of Federal Regulation, Parts 5 and 736.

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)?**	During the hiring process, SPR collects mandatory information from employees. To be granted access to SPR facilities, the applicant must provide all required personal information and go through the background investigation. Most information obtained during the hiring process is not voluntary but is only used for authorized business purposes.
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
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed PSMA 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 the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. PSMA 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 • Limited physical and logical access to this system PSMA contains some PII, the ensuing risk to the privacy of individuals is generally moderate given the type of information that is retrieved. Technical, physical, and administrative controls are used to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. Data is only used by authorized personnel for authorized business purposes. The system also has had a full certification and accreditation.

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 can be retrieved by using the following identifiers: name, date of birth, badge number, and employment status.
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 Federal Register, Vol. 74, No. 6, Friday, January 9, 2009 Energy Department, Privacy Act; System of Records DOE-63 Personal Identity Verification (PIV) Files
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?	Data is collected by a Personal Identity Verification (PIV) authorized agency, along with SPR security specialists.
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?	Yes, at the business application level.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	The protected PII is used by DOE employees and contractors for physical access control.
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?	Personnel security staff can generate reports that show access times of employees with PIV cards.
15. What will be the use of these reports?	Management will use the reports for oversight of employee entry and exit at SPR facilities.
16. Who will have access to these reports?	Personnel security, system administrators, and cyber security.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The information system is used to identify employees upon entry to an SPR facility. It will also be able to determine if an employee is presently located within an SPR facility, however, it does not provide the capability to locate an employee within the facilities.
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?	YES
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.	All data is user provided and is part of the PIV card issuance process. Personnel security staff use internal controls and processes to ensure data currency. PIV card re-issue keeps data current. Also, the SPR badging system maintains a list of authorized personnel and is updated when an employee is terminated. The employee list is pushed out nightly and SPR personnel must compare it to the badging 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?	The SPR PSMA is operated at all five (5) SPR sites. Only trained security force, administrators, and cyber security personnel will be able to access the information system at any site. Automated database synchronization keeps system data consistent between sites.
Records Management	
22. Identify the record(s).	The Sitewide Card Access System is the only system on PSMA that has PII. Name and birthdate are the only PII stored. Entry control processing into the main gates and into the buildings at the sites based on the status of PIV application (can get in main gate vs. access buildings based on application status). Records are access control information into the SPR physical sites
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The Sitewide Card Access System is treated as a system of record and as such, the information within is not disposed of individually. Unscheduled X Scheduled *(cite NARA authority(ies) below)* GRS 5.6 Item 090
24. Records Contact	Sarah Lambert-Sheffield **Sarah.Lambert-sheffield@spr.doe.gov** (504) 734-4225
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and procedural controls as defined in the SSP protect the data on this information system. In addition, there is limited physical and logical access to this system.
26. Who will have access to PII data?	Security specialists and system administrators are the only personnel allowed to access or modify data in the course of their official duties. Cyber Security provides oversight of the information system.

MODULE II – PII SYSTEMS & PROJECTS

27. How is access to PII data determined?	User's access is restricted based on the functional role, user account, and data required to perform official duties.
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?	N/A, PII data is not shared with any connecting system.
30. Who is responsible for ensuring the authorized use of personal information?	System Owner

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) DAWN GLAPION Digitally signed by DAWN GLAPION Date: 2022.07.26 12:33:23 -05'00' (Signature)	
Local Privacy Act Officer	(Print Name) KRISTIN FRISCHHERTZ Digitally signed by KRISTIN FRISCHHERTZ Date: 2022.07.21 13:23:55 -05'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2022.07.20 15:58:42 -04'00' (Signature)	