Affects Members Of the Public? ☐

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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

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	7/17/2017	
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE), Golden Field Office (GFO)	
Name of Information System or IT Project	GFO Light Weight Credentialing Station	
Exhibit Project UID	N/A	
New PIA ☒ **Update** ☐	This is a new PIA for GFO Light Credentialing Stations (LCS)	
	Name, Title	**Contact Information Phone, Email**
System Owner	Chris Mullane, Security & Emergency Manager	240-562-1728 christopher.mullane@ee.doe.gov
Local Privacy Act Officer	Michele Altieri, Golden Field Office, Privacy Act Officer	240-562-1427 michele.altieri@ee.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	**Judith Tegeler, Golden Field Office, Cyber Security Manager**	**240-562-1366** **judith.tegeler@ee.doe.gov**
Person Completing this Document	**Chris Mullane**	
Purpose of Information System or IT Project	**The Golden Light Credentialing Solution (LCS) implements Identity, Credential, and Access Management (ICAM) requirements (DOE O 206.2) and administers long range HSPD-12 badges to all GFO staff. This is a GSA owned station that is issued to GFO to issue PIV badges as required by HSPD-12. The LCS acts as a conduit for information to be transferred to USAccess which is owned and protected by the GSA. All electronic transactions are done via this GSA system. Any paper forms that are used during sponsorship are shredded.**	
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 ☐ Other – Please Specify	
Has there been any attempt to verify PII does not exist on the system?		**N/A**

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	**N/A**
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	**Yes, this system collects information about individuals.**
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?	(If Yes, select with an "X" in the boxes below) ☒ 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 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?**	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 Regulations, Part 5 and 736.
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)?**	DOE published System of Records Notice, DOE-63. The information collected is required documentation to support the HSPD-12 PIV badging. No personnel information, other than the minimum required, is collected for this purpose.
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 may be involved in the day to day use of the system. Contractors will have the appropriate CRD and privacy clauses included in their contracts. Contractors will help to enroll and activate user's badges.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	**The impact of the LCS is moderate due to the sensitivity of the information. This risk is mitigated by the following.** • **The LCS access the USAccess database which is owned and operated by GSA.** • **The LCS provides only the tools, fingerprint scanner, camera, and document scanner to submit the appropriate information to USAccess.** • **Digital information is not stored locally, only paper copies that are destroyed once the new employee has been adjudicated.** • **The paper copies remain in a locked cabinet in a locked room that is in a building that is monitored 24/7 until destruction**
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 paper copies are retrieved by name. All digital information is housed in a GSA or OPM system that has approved privacy controls in place. Electronic records are pulled by name from the GSA owned and operated system.**
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 63 of the DOE SORN states, "The records maintained in this system of records include all documents submitted during application for the PIV credential or copies of those documents, and any resulting investigative, adjudicative, appeal, or reciprocity documentation."**

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?	NO
8. What are the sources of information about individuals in the information system or project?	Users supply the information. The credentialing system pulls records by name to include any and all information contained in the GSA system.
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
11. How will the PII be used?	The information will be used in accordance with Homeland Security Presidential Directive 12 (HSPD-12) issued on August 27, 2004 regarding the establishment of a standard for identification of Federal Government employees and contractors. *See also*, "Routine Uses" in DOE SORN, DOE-63 "Personal Identity Verification (PIV)". Information is used to allow for the creation or transfer of certificates to the PIV card.
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. The system will not derive metadata.
13. With what other agencies or entities will an individual's information be shared?	GSA houses and maintains the information collected.

MODULE II – PII SYSTEMS & PROJECTS

14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are generated from the LCS.
15. What will be the use of these reports?	No reports are generated from the LCS
16. Who will have access to these reports?	No reports are generated from the LCS
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. No digital information is stored locally. The systems that connect to GSA USAccess is in a locked room in a monitored building. All paper files are kept in a locked cabinet in a locked room in a monitored building and cannot be used to locate or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	Individuals are not monitored.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. No digital information is stored locally. The system that connect to GSA USAccess is in a locked room in a monitored building. All paper files are kept in a locked cabinet in a locked room in a monitored building and cannot be used to locate or monitor individuals. All digital information is housed in a GSA system that has approved privacy controls in place.
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.	NA. Paper copies are destroyed after the individual is adjudicated. If erroneous information is found a correction is submitted to GSA.

MODULE II – PII SYSTEMS & PROJECTS

21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	All digital information is housed in a GSA system that has approved privacy controls in place.
Records Management	
22. Identify the record(s).	Biographic and biometric information. *See also*, DOE SORN, DOE-63, "Categories of Records in the System."
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Records relating to security clearance/access authorization are scheduled IAW N1-434-03-01, item 22 and DOE ARM 18 (Rev 2), item 22
24. Records Contact	Michele Altieri, michele.altieri@ee.doe.gov, 720-454-8868
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	All paper files are kept in a locked cabinet in a locked room in a monitored building. Only approved sponsor, adjudicator, and activator have access to information. All digital information is housed in a GSA system that has approved privacy controls in place.
26. Who will have access to PII data?	The GSA USACCESS approved Sponsor, Adjudicator, Reroller/Activator have access for the purpose of creating a PIV badge
27. How is access to PII data determined?	Authorized users must complete USAccess role based training and the positions must be approved by DOE HQ Security AU-72
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. AU-72 manages any agreements associated with this system.

MODULE II – PII SYSTEMS & PROJECTS	
30. Who is responsible for ensuring the authorized use of personal information?	**The Golden Field Office Security Manager.**
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	___Chris Mullane_______________________ (Print Name) _______________________ (Signature)	7/17/17
Local Privacy Act Officer	___Michele Altieri_______________ (Print Name) Michele Altieri (Signature)	17 July 17
Chief Privacy Officer	_______________________ (Print Name) _______________________ (Signature)	_______________