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: 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	January 31, 2017	
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy, Golden Field Office, National Renewable Energy Laboratory	
Name of Information System or IT Project	NREL Computing System – NREL Access Control Program and Foreign National Management Program.	
Exhibit Project UID	DOE Contract DE-AC36-08GO28308.	
New PIA □ **Update** ☒	This is an annual update for the NREL 2017 – Access Control and FN Management PIA	
	Name, Title	**Contact Information Phone, Email**
System Owner	NREL Access Control Program (Personnel Security, Long and Short Term Badging). Joe Thill, Director, Office of Security and Emergency Preparedness Foreign National Management – Pamela Missett, Deployed Human Resources and Talent Acquisition Manager	303-275-4645 Joe.Thill@nrel.gov 303-384-7596 Pamela.Missett@nrel.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Michele Altieri, Golden Field Office, Privacy Act Officer	720-356-1427 Michele.Altieri@ee.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Bob Gladu, NREL ISSO	303-275-4009 Bob.Gladu@nrel.gov
Person Completing this Document	Bob Gladu, NREL ISSO Kaycee Edwards, Mission Support Group Manager Viktoriya Esayev, Foreign National Access Administrator	303-275-4009 Bob.Gladu@nrel.gov 303-275-3702 Kaycee.Edwards@nrel.gov 303-275-4269 Viktoriya.Esayev @nrel.gov
Purpose of Information System or IT Project	The NREL Access Control program implements Personnel Security requirements (DOE O 472.2) and administers both Long and Short term badges to all personnel entering the National Renewable Energy Laboratory or any of its remote sites. The Site Access database documents management authorized access for Site Physical area access. The Foreign National Management system is used to document all Foreign National access to the National Renewable Energy Laboratory or any of its remote sites.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify (Country of Citizenship, Place of Birth, Picture)
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.*	N/A
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

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 ☒ 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

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	U.S. Department of Energy Contract No. DE-AC36-08GO28308. As provided in DOE O 206.1, "The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President." Information collected under Personnel Security does not exceed that which is specifically required by DOE O 472.2, Personnel Security. DOE O 142.3A Unclassified Foreign Visits and Assignments Program

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)?**	The information collected is required documentation to support access to the National Renewable Energy Laboratory and its remote sites. No personal 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?**	Yes. Yes.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Use of the information in the Access Control program and Foreign National Management system is not expected to impact privacy of the individuals involved.
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 data is primarily retrieved using the individual's name. The information is in both electronic and hard copy format.

MODULE II – PII SYSTEMS & PROJECTS

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 51, Employee and Visitor Access Control Records; DOE-52, and Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites. Federal Register, Vol. 74, No. 6, Friday, January 9, 2009.
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?	User supplied information in the form of visitor form submissions, presented identification verification, Driver's License, government ID, proof of citizenship, visa and Permanent Resident Alien card.
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. Support documentation exists for these systems.
DATA USE	
11. How will the PII be used?	Visitor Information will be used to meet all DOE documentation and validation requirements for Visitors to NREL. The badging information will be used to produce permanent badges in accordance with DOE requirements. FN Management – The information is used validate identity, authority to work status, and lawful immigration status.

MODULE II – PII SYSTEMS & PROJECTS

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?	None.
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 badging system will be able to collect limited information about users from badge readers when the users are on site.
18. What kinds of information are collected as a function of the monitoring of individuals?	Badge reader entries show time and date that a badge is read. Information is only collected when entering the site or entering an area that has restricted access enforced. There are no area or site exit badge reader requirements.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. All individual monitoring requests must be explicitly approved by Human Resources and senior management.

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.	Badging System - Most of the records are not updated after initial submission and processing for initial collection. If needed, information is updated for future requests and resubmissions. FN Management – All supplied documents are updated prior to their expiration.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A
Records Management	
22. Identify the record(s).	Badging system data is retained for 2 years. Foreign National Management Data (in hard copy) is retained for 5 years. Copies of all documents required to verify the foreign national's identity, authority to work, and lawful immigration status e.g. FN Data Card, visa, Permanent Alien Resident Card, passport. These forms and database entries are deleted manually by application and Program administrators. Electronic records are disposed of by following detailed procedures to ensure all data is sanitized or destroyed during end of life processing for systems and storage devices. Paper records are destroyed by putting them in locked disposal bins that are shredded on site by a contracted shredding company.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Access Control Program: ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* Visitor Control Files, NARA records schedule authority N1-434-98-21, Item 17.b Foreign National Program: ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* Incident of Security Concern Inquiry/Investigation Files, NARA records schedule authority N1-434-98-21, Item 11.3

MODULE II – PII SYSTEMS & PROJECTS

24. Records Contact	Lee Michael, Records Management Manager lee.michael@nrel.gov, 303-275-4213
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The NREL computing environment, which contains both the Access Control Program and paper documentation for the Foreign National Management Program, is accredited to process FIPS-199 (February 2004) categorized information at the Moderate level. The accreditation was granted on December 20, 2013 and is in effect until August 20, 2017. All baseline security controls were tested as a part of the certification and accreditation process and risks were mitigated to an acceptable level as approved of by the Authorizing Official. The accreditation was based on NIST 800-53R3 (August 2009) security controls and the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy (EERE) Program Security Plan Version 2.4 (June 2012).
26. Who will have access to PII data?	Access Control Program – There are 9 Security system administrators with access to this information. Roles include: Security management (1) Security support (3) IT administration (3) Vendor on site access (2) Foreign National Management Program – All authorized FACTS users.
27. How is access to PII data determined?	Access Control Program – Access is granted based on roles and is approved by the Director, Security and Emergency Preparedness Foreign National Management Program – Explicit access on a case by case basis by the Foreign National Management Program Administrator.

MODULE II – PII SYSTEMS & PROJECTS	
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.
30. Who is responsible for ensuring the authorized use of personal information?	Joseph Thill - Director, Security and Emergency Preparedness. Pamela Missett – Deployed Human Resources and Talent Acquisition Manager

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	Joe Thill (Print Name) Director, Office of Security and Emergency Preparedness (Signature)	4-6-17
	Pamela Missett (Print Name) Deployed Human Resources and Talent Acquisition Manager Pamela Missett (Signature)	4/6/17
Local Privacy Act Officer	Michele Altieri, Golden Field Office (Print Name) Michele Altieri (Signature)	6 Apr 2017
Chief Privacy Officer	(Print Name) (Signature)	