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	4/26/2017
Departmental Element & Site	Office of Energy Efficiency and Renewable Energy (EERE), Golden Field Office (GFO)
Name of Information System or IT Project	GFO Personnel Security Files
Exhibit Project UID	N/A
New PIA X **Update**	This is a new PIA for Personnel Security Files.

	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
Cyber Security Expert reviewing this	Judith Tegeler, Cyber Security Manager	240-562-1366 judith.tegeler@ee.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	**Chris Mullane**	**240-562-1728** **Christopher.mullane@ee.doe.gov**
Purpose of Information System or IT Project	**The purpose of this system is to establish an entry into several non-DOE managed databases to assess the person's suitability for employment.**	
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? **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*		**N/A**

MODULE I – PRIVACY NEEDS ASSESSMENT

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**
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?	(If Yes, select with an "X" in the boxes below) ☒ 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.

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*,; 10 CFR Part 710, Subpart A; Executive Orders 10450 and 12968; 5 CFR Part 732; DOE O 474.4 Safeguards and Security Program of 8-26-05; DOE M 470.4-5, Personnel Security, of 08-26-05 and Director of Central Intelligence Directive 6/14 of 6-20-00.**
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-43. The information collected is required documentation to support the personnel security program. Only the minimum amount of information that is 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?**	**No**

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	**The potential impact is moderate due to the amount and nature of the data. The loss of confidentiality, integrity, or availability are mitigated by the following:** • **No digital copies of information are stored locally. Any digital information is input directly into a system owned and operated by GSA, FBI, and/or OPM and under approved privacy controls.** • **Only paper copies are retained locally. These paper copies reside in a locked file cabinet which is located in a locked room in a controlled facility with 24/7 monitoring.** • **Paper copies are stored in a locked cabinet in a locked room in a building that is monitored 24/7.** • **The records that are created in other federal databases are protected according to applicable federal policies and laws.**
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 are retrieved using names, SSNs, and DOB. Access to the information is limited to only those with a role based authority to access said data. The data are housed in other federal agency databases and accessed via a secure portal which follows FIPS standards.**
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 43 of the DOE SORN states, "For those records described in *Categories of Records in the System,* such records are maintained and used by the Department as an official record of all information gathered and evaluated to determine an individual's initial and continued DOE access authorization eligibility and, if applicable, an individual's eligibility for participation in DOE sensitive activities or for access to Sensitive Compartmented Information."**

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?	Information is supplied by the individual onto a paper form. This data is then input via secure connection to eQIP, which is owned and operated by the OPM. Paper copies of fingerprints are not stored. eQIP is used to process electronic questionnaires for investigative processing for federal security, suitability, fitness, and credentialing purposes.
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 background investigation information will be used in accordance with DOE requirements, see for example DOE O 474.4 Safeguards and Security Program of 8-26-05; DOE M 470.4-5, Personnel Security, of 08-26-05. See also, "Routine Uses" DOE SORN, DOE-43 "Personnel Security Files"** **From the SORN: Purposes: For those records described in Categories of Records in the System, such records are maintained and used by the Department as an official record of all information gathered and evaluated to determine an individual's initial and continued DOE access authorization eligibility and, if applicable, an individual's eligibility for participation in DOE sensitive activities or for access to Sensitive Compartmented Information.** **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:** **1. A record from this system may be disclosed as a routine use to competent medical authority who, under a formal agreement for payment of services with the local DOE personnel security element, conducts evaluations under Title 10, Code of Federal Regulations, Part 710, to determine whether an individual has an illness or mental condition of a nature which causes, or may cause, a significant defect in judgment or reliability, or is alcohol dependent or suffering from alcohol abuse.** **2. A record from the system may be disclosed as a routine use to a federal, state, or local agency to obtain information relevant to a Departmental decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit. The Department must deem such disclosure to be compatible with the purpose for which the Department collected the**

	information. 3. A record from this system may be disclosed to a federal agency to facilitate the requesting agency's decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. The Department must deem such disclosure to be compatible with the purpose for which the Department collected the information. 4. A record from the system may be disclosed as a routine use to the appropriate local, state or federal agency when records alone or in conjunction with other information, indicates a violation or potential violation of law whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program pursuant thereto. 5. A record from this system of records may be disclosed to a member of Congress submitting a request involving the constituent when the constituent has requested assistance from the member with respect to the subject matter of the record. The member of Congress must provide a copy of the constituent's request for assistance. 6. A record from this system of records may be disclosed to foreign governments or international organizations in accordance with treaties, international conventions, or executive agreements 7. A record from the system may be disclosed as a routine use to DOE contractors in performance of their contracts, and their officers and employees who have a need for the

MODULE II – PII SYSTEMS & PROJECTS	
	record in the performance of their duties. Those provided information under this routine use are subject to the same limitations applicable to Department officers and employees under the Privacy Act. 8. A record from this system may be disclosed as a routine use when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security integrity if this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
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?	**The information is submitted to systems that are owned and operated by the FBI and OPM that are subject to federal privacy controls.**

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are produced from these paper copies. A paper document with basic information about the user is kept in a locked file cabinet which is located in a locked room in a controlled facility with 24/7 monitoring.
15. What will be the use of these reports?	No reports are produced.
16. Who will have access to these reports?	No reports are produced
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No, the system will not have the capability to identify, locate, and 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?	The following controls are in place to prevent unauthorized access to include monitoring of individuals: • No digital copies of fingerprints are stored locally. All digital data is housed in a GSA or OPM system that has approved privacy controls in place. • Only paper copies are retained locally. These paper copies reside in a locked file cabinet which is located in a locked room in a controlled facility with 24/7 monitoring. • Digital information is submitted via secure portal to other agencies (GSA USAccess, FBI, and/or OPM) and stored on systems that have approved privacy controls in place.

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.	NA. Paper copies are destroyed after the individual is adjudicated.
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 information is provided by the individual and verified against other information kept by OPM. Information is transferred to OPM but not received from them, so there is no way for the information to be inaccurate.
Records Management	
22. Identify the record(s).	Pre-employment background files including records of investigations and security clearance/access authorization case records. *See also*, DOE SORN, DOE-43, "Categories of Records in the System."
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Pre-employment background files: Scheduled IAW N1-434-98-21, item 21.3 and DOE ARM 18 (Rev 2), item 21.3 Security clearance/access authorization case records: 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 720-356-1427
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	All information is kept in a locked cabinet in a locked room in a building monitored 24/7.
26. Who will have access to PII data?	The GFO Security Office.
27. How is access to PII data determined?	Only GFO security personnel are permitted to have access to this 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.	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?	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) (Signature)	17 July 17
Chief Privacy Officer	(Print Name) (Signature)	