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 electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	August 27, 2009
Departmental Element & Site	Office of the Chief Information Officer DOE Headquarters, Forrestal, 8H-065
Name of Information System or IT Project	HSPD-12 Physical and Logical Access System
Exhibit Project UID	**Project's Unique ID: 019-60-01-17-01-8062-04-404-140 (2010 UID)**
New PIA ☐ **Update** X	HSPD-12 Physical and Logical Access System

	Name, Title	Contact Information Phone, Email
System Owner	Frederick A. Catoe	Phone: 301-903-6453 frederick.catoe@hq.doe.gov
Local Privacy Act Officer		
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Paul R. Aaron, CISA,PMP	(202) 586-0847 Paul.aaron@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Paul R. Aaron, CISA,PMP	(202) 586-0847 Paul.aaron@hq.doe.gov
Purpose of Information System or IT Project	The purpose of the system is to establish a standards-based authentication and authorization infrastructure. In order to comply with the authentication requirements of **Federal Information Processing Standards Publication 201** (FIPS 201), the identity of an individual must be established before issuing that individual a **Personal Identity Verification** (PIV) Card. All of the data contained in the system is designed for one purpose only: to positively and accurately verify that a person is, in fact, who he/she claims to be. The Applicant completes and submits appropriate background investigation forms to the Registrar. The Applicant then provides two identity source documents listed in Form I-9 (Employment Eligibility Verification) to the Registrar. One of these forms will be a State or Federal Government-issued picture identification. The Registrar will verify the validity of the documents and compare the picture on the identity source document with the Applicant to confirm the identity of the Applicant. The Registrar will then record[1] the document title, document issuing authority, document number, and document expiration date (if any) for both identity source documents. The Registrar also ensures the collection of fingerprints and a photograph of the individual.	
Type of Information Collected or Maintained by the System:	X SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" X Biometric Information e.g. finger print, retinal scan X Maiden Name if applicable X DoB, Place of Birth X Name, Phone, Address	

MODULE I – PRIVACY NEEDS ASSESSMENT

	X Other – Document number from the identity source documents. May include military status; foreign national status; federal emergency response official status; law enforcement official status; results of a background check; and PIV Card issuance location.

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.*	NO
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 X Federal Employees X 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?**	**Homeland Security Presidential Directive/HSPD-12** dated August 27· 2004 **Federal Information Processing Standards (FIPS 201) dated February 2005**
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)?**	Information is voluntary. Applicant can decline, however they will not receive a PIV Card.

MODULE II – PII SYSTEMS & PROJECTS	
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 DOE Notice 206.4 addresses the CRD.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	YES A significant compromise of this system including its PII information could be expected to have a moderate impact.
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.**	YES GSA/GOVT -7 Personal Identity Verification Management System (PIV IDMS)
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*.**	This information is covered by the government-wide system of records. GSA/GOVT -7 Personal Identity Verification Management System (PIV IDMS)

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Information will obtained from individuals applying for the PIV Card, The PIV IDMS records will cover all participating Federal employees, contractors, and volunteers who require routine, long-term access to Federal facilities, IT systems, and networks. The system also includes individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.). It is the Department's discretion to include short-term (working in a Federal facility for less than six months) employees and contractors in the PIV Program and, therefore, inclusion in the PIV IDMS. DOE will make risk-based decisions to determine whether to issue PIV Cards and require prerequisite background checks for short-term employees and contractors. The system does not apply to occasional visitors or short-term guests. DOE will issue temporary identification and credentials for this purpose.
9. Are the data elements described in detail and documented?	Yes, the data elements are described in detail, and are documented in the GSA System Security Plan (SSP), Appendix D, Security Categorization.
DATA USE	
10. How will the PII be used?	The data will be use to complete the identity proofing and registration process.

MODULE II – PII SYSTEMS & PROJECTS

11. With what other agencies or entities will an individual's information be shared?	The GSA Shared Service Provider. The exception is disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act. All or a portion of the records or information contained in this system may be disclosed outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: A. To the Department of Justice (DOJ) when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records. B. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records. C. Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity. D. OPM.

MODULE II – PII SYSTEMS & PROJECTS

Reports	
12. What kinds of reports are produced about individuals or contain an individual's data?	N/A
13. What will be the use of these reports?	N/A.
14. Who will have access to these reports?	N/A
Monitoring	
15. Will this information system provide the capability to identify, locate, and monitor individuals?	No Monitoring
16. What kinds of information are collected as a function of the monitoring of individuals?	N/A
17. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
DATA MANAGEMENT & MAINTENANCE	
18. 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.	The data is submitted by the individual from whom it pertains, therefore the information is accurate, relevant and complete at the time the data is submitted.
19. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The Physical system is operated at one site which is the GSA USAccess site.
Retention & Disposition	

MODULE II – PII SYSTEMS & PROJECTS	
20. What are the retention periods of data in the information system?	Information will be retained according to DOE Administrative records Schedule II: Space and Administrative records dated 12/22/00.
21. What are the procedures for disposition of the data at the end of the retention period?	According to DOE Administrative records Schedule II: Space and Administrative records dated 12/22/00, these records will be destroyed after appropriately accounting for the PIV card.
ACCESS, SAFEGUARDS & SECURITY	
22. What controls are in place to protect the data from unauthorized access, modification or use?	The GSA MSO USAccess protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards: System Security: These controls include network security and limited access to system and physical facilities. System risks are addressed by the SSP and Risk Assessment established for this PIV Program. More specific program controls include protecting data through the use of FIPS validated cryptographic algorithms in transit, processing, and at rest. Networks: The IT infrastructure that supports the PIV Program is described in detail in the GSA SSP. All data exchange takes place over encrypted data communication networks that are designed and managed specifically to meet the needs of the PIV Program. Private networks and/or encryption technologies are used during the electronic transfer of information to ensure "eavesdropping" is not allowed and that data is sent only to its intended destination and to an authorized user, by an authorized user. Enrollment data may be temporarily stored at enrollment centers for encrypted batch transmission to the PIV IDMS. Access is PIN protected. DOE Logical Access protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards uses network security to protect Personal Identifiable Information (PII) by the inherent security of the system (i.e., firewalls, passwords, cryptographic logon, and separation of roles).

MODULE II – PII SYSTEMS & PROJECTS

23. Who will have access to PII data?	Access to the data is strictly controlled, and is limited to those with an operational need to access the information. There are three core sets of user population: 1. Users with administrative and operational responsibilities (e.g., Agency Security Officers) (hereinafter "administrative personnel") 2. Users who are provided access to the GSA MSO USAccess system and its applications (e.g., Sponsors, Registrars, and Adjudicators) (hereinafter "privileged users") 3. GSA MSO USAccess applicants (hereinafter "general users"). Administrative personnel and privileged users are subject to rigorous background checks before they are allowed access to the system.
24. How is access to PII data determined?	A "least-privilege" role-based access system restricts access to data on a "need-to-know" basis. Only a select few administrative and privileged users will have access to all the data, and these individuals undergo a rigorous background screening process.
25. Do other information systems share data or have access to the data in the system? If yes, explain.	NO, Federal agencies will only have access to their own particular agency's data (not to any other agency's data).
26. 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?	Yes, The interconnection between the General Services Administration and the DOE are for the expressed purposes of using the GSA HSPD-12 Shared Services Solution, consisting of Enrollment/Activation Stations (EAS) for sending data (i.e., scanned fingerprint images with authentication information) to request issue of PIV Credentials for government and contractor employees as required by HSPD-12, and for the GSA HSPD-12 Shared Solution infrastructure to obtain data (i.e., software updates, encryption, configuration).
27. Who is responsible for ensuring the authorized use of personal information?	The GSA MSO Program Manager is responsible for protecting the privacy rights of the individuals affected by the interface. Individuals with a role identified or defined in the system GSA MSO USAccess *PCI Operations Plan* are also responsible for protecting the privacy rights of individuals (e.g., Sponsors, Registrars, Agency Privacy Officials). For logical access the DAA for DOE.

END OF MODULE II

SIGNATURE PAGE		
	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	