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: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	April 7, 2022
Departmental Element & Site	Office of the Executive Secretariat, MA-73 Office of Management U.S. Department of Energy DOE Headquarters, Forrestal HOSTED with the Energy IT Services (EITS) Data Center & System Services (DC&SS). The facility is located in the Culpepper, Virginia
Name of Information System or IT Project	Subsystem: Electronic Document Online Correspondence and Concurrence System (eDOCS) Enclave: EITS Hosted/MA Applications Enclave
Exhibit Project UID	019-60-01-17-02-3019-00-404-141.
New PIA ☐ **Update** X	April 2019

	Name, Title	Contact Information Phone, Email
System Owner	Shena A. Kennerly Office of the Executive Secretariat, MA-73	202-586-0577 Shena.Blake-Kennerly@hq.doe.gov
Local Privacy Act Officer	Ilir Angjeli Office of Corporate Business Operations, MA-1.1	(202) 586-3282 Ilir.Angjeli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ilir Angjeli, ISSM Office of Corporate Business Operations, MA-1.1	(202) 586-3282 Ilir.Angjeli@hq.doe.gov
Person Completing this Document	Shena A. Kennerly Office of the Executive Secretariat, MA-73	202-586-0577 Shena.Blake-Kennerly@hq.doe.gov
Purpose of Information System or IT Project	The primary purpose of eDOCS is to serve as a tool to manage and control 1) correspondence to and from the Secretary of Energy through the Office of the Executive Secretariat (EXECSEC), 2) correspondence to and from Freedom of Information Act (FOIA) and Privacy Act (PA) requesters, and 3) information about members of DOE Advisory Committees. Correspondence may be received and sent to members of Congress, the White House, Federal government agencies, State and Local government agencies, other DOE program offices, and the general public. eDOCS provides an efficient electronic document management system and a workflow process that ensures that correspondence is addressed in a timely manner. The system also provides a records-management system that stores records in accordance with mandated retention periods. An encrypted subset of eDOCS is also used to store DOE employee records and changes to their records, which may contain personal information in an "identifiable form." The records are passively archived in the system and read-access is allowed only to authorized individuals.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify The following information is collected from the public: name, home and work address, home and work telephone number, personal and work electronic mail address, type of business or organizational affiliation, a description of the records requested, and a description of matters for DOE consideration or resolution.
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 ☒ 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 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?**	• Department of Energy Authorization Act, Title 42, United States Code (U.S.C.), Section 7101 et. seq.; • Department of Energy Authorization Act, Title 50, United States Code (U.S.C.), Section 2401 et. seq.; • Freedom of Information Act, 5 U.S.C. 552; • Privacy Act, 5 U.S.C. 552a.
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 personal information stored in the system about members of the public is required in order for DOE to respond to their requests and to Congressional requests on behalf of constituents. Information submitted by members of the public is voluntarily provided. Information submitted by DOE Advisory Committees members is voluntarily provided. The information is used by DOE for the purpose of maintaining a complete and accurate listing of all Advisory Committee members.

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?**	Contractors are involved in the design, development, and maintenance of the system. Personal information from eDOCS may be disclosed to these contractors and their officers and employees in performance of their contracts. Those individuals who are provided this information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need–to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and requirements of DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	There may be significant risk to privacy if the system is compromised. The accidental disclosure of PII in the system may negatively impact individuals if their personal information is made public potentially resulting in personal embarrassment, professional harm, and damage to the trust between members of the public and the Federal Government. The degree of harm potential depends on the sensitivity of the information which varies depending on the request; accordingly, the potential harm to an individual may be minimal or significant. However, eDOCS, a DOE intranet-based application, protects data through multiple security controls to mitigate the risk of compromise. The security controls of the system are reviewed annually as part of the Assessment & Authorization process that addresses the National Institute of Science and Technology (NIST) 800-53 Rev.4, Security and Privacy Controls for Information Systems and Organizations controls and ensures the application is compliant with Federal and DOE policies. eDOCS limits access to only DOE authorized users. eDOCS uses Active Directory (AD) to manage and authenticate HQ users and groups. The system leverages the Enterprise DOE domain managed by the OCIO for account authentication and security policies. DOE HQ users must first login to DOE Network using PIV/HSPD-12 authentication. Then authorized eDOCS users must authenticate to the application through the use of password-based authentication managed and controlled by the system administrator. For lab and field site users to login to the application, the eDOCS application leverages OneID which provides identity management and PIV/HSPD-12 authentication for all DOE personnel. Rules of Behavior are signed by the authorized users before gaining access to the system and the consequences for violating DOE rules are displayed and acknowledged at system logon. eDOCS protects the confidentiality and integrity of information at rest through encryption at the server/operating system layer. The system has been designed to provide the capability to compile audit records from multiple components throughout the system in a logical, time-correlated audit trail if a compromise is suspected.

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 is retrieved by name, control number and other non-PII data fields which are populated based on information from the document. In the encrypted eDOCS repository, data is retrieved by social security number by a limited number of authorized users.
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*.**	The system operates in accordance with the following DOE Systems of Records (SORs): • DOE-9 Members of DOE Advisory Committees • DOE-55 Freedom of Information and Privacy Act (FOIA/PA) Requests for Records • DOE-56 Congressional Constituent Inquiries • DOE-58 General Correspondence Files of the Secretary, Deputy Secretary and Under Secretary of Energy http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=38820&dbname=2003_register
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No, the system is not being modified.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The information is obtained from the individual to whom it pertains.
9. Will the information system derive new or meta data about an individual from the information collected?	No, the information system does not derive new or meta data about an individual.

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	Data elements are described in the following documentation: Department of Energy Electronic Correspondence and Concurrence System, Functional Requirements Document, Rev. 4, March 1, 2005 and Department of Energy Electronic Correspondence and Concurrence System, Detailed System Design Document, Rev. 4, March 1, 2005. The data elements are reviewed annually.
DATA USE	
11. How will the PII be used?	All data in the system is relevant and necessary for DOE to perform its required correspondence, FOIA, and PA responsibilities. The personal information stored in the system about members of the public is required in order for DOE to respond to their requests and to Congressional requests on behalf of constituents.
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?**	The system will not use or derive new or meta data.
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?	No reports are produced on individuals.
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 system will not use tools or other methods to identify, locate or monitor individuals.

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	The system does not monitor individuals.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	The system does not monitor individuals. eDOCS limits access to only DOE authorized users which must authenticate through the use of password-based authentication managed and controlled by the system administrator. Rules of Behavior are signed by the authorized users before gaining access to the system and the consequences for violating DOE rules are displayed and acknowledged at system logon. eDOCS protects the confidentiality and integrity of information at rest through encryption at the server/operating system layer. The system has been designed to provide the capability to compile audit records from multiple components throughout the system in a logical, time-correlated audit trail if a compromise is suspected. The security controls of the system are reviewed annually as part of the Assessment & Authorization process that addresses the National Institute of Science and Technology (NIST) 800-53 Rev.4, Security and Privacy Controls for Information Systems and Organizations controls and ensures the application is compliant with Federal and DOE policies.
DATA MANAGEMENT & MAINTENANCE	
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.	eDOCS does not verify the accuracy or completeness of the data related to the general public.The data in the system is provided by the individual to whom it pertains. Therefore, it is determined that the information is accurate, timely, and complete at the time it is provided.
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 system is operated at DOE Headquarters only and accessed by authorized users from the DOE Headquarters. The system is hosted by the DOE Office of the Chief Information Officer (OCIO).
Records Management	
22. Identify the record(s).	There are no retention or disposition schedules in the system. The correspondence items stored in eDOCS must be retained forever as mandated by federal policy.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ **Unscheduled** □ Scheduled (cite NARA authority(ies) below) N/A
24. Records Contact	Shena A. Kennerly Office of the Executive Secretariat, MA-73 202-586-0577 Shena.Blake-Kennerly@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The System Owner has implemented and tested all moderate baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via user-id and password based on user responsibility and job function. These access controls are defined in Section 4 of the eDOCS SSP. All system team members (federal and contractor) are required to complete the DOE Headquarters Annual Cyber Security Refresher Briefing as a necessary prerequisite for access to the system. Rules of Behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, separation of duties so individuals only have access to the personal information needed to perform duties, and use of system audit logs to monitor access and user activity in the system. In addition, Documentum Trusted Content Services (TCS) was implemented. TCS provides an extra layer of security and complements the core security features of Documentum Content Server. TCS is deeply embedded within the server and includes Repository Encryption, Electronic Signatures, Multi-dimensional access control (MAC), and Digital Shredding. All eDOCS repositories use the encryption features to encrypt the content files at rest. Repository encryption uses the 3DES-CBC encryption algorithm with a 192-bit key length. Content encryption is seamless to the users, DCTM encrypts/decrypts behind the scenes. Note: EMC licenses all encryption algorithms from RSA Security.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Only authorized DOE federal and contractor personnel have access to the data in the system. Access to personal data in the system will be strictly controlled based on job responsibility and function. The Access Control List is available from the System Owner.
27. How is access to PII data determined?	Access to data is determined by evaluation of job responsibilities and organization. Based on the evaluation, the user is assigned permissions that are applied using system access control lists. User accounts are reviewed semiannually to identify and remove users who have left the organization or whose duties no longer require access to the system.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No other systems share PII data or have access to the PII data in the system.
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?	Yes. eDOCS has authorized connections with three (3) other information systems (the Energy Efficiency and Renewable Energy Executive Information System (EERE) DW 2.0, Energy.gov, and the Loan Program (LP) Quicksilver) with interconnection security agreements.
30. Who is responsible for ensuring the authorized use of personal information?	The system owner is responsible for ensuring the authorized use of personal information.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Shena Kennerly** (Print Name) (Signature)	
Local Privacy Act Officer	**Ilir Angjeli** (Print Name) (Signature)	
Chief Privacy Officer	**Ken Hunt** (Print Name) (Signature)	