Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	September 1, 2021
Departmental Element & Site	Office of Public Information, Office of Administration Office of Management DOE Headquarters, Forrestal
Name of Information System or IT Project	FOIAXpress (Freedom of Information Act)
Exhibit Project UID	019-60-01-17-02-3045-00
New PIA ☐ **Update** X	This PIA updates a PIA approved on October 1, 2018. This update documents new improvements to the FOIAXpress system.

	Name, Title	Contact Information Phone, Email
System Owner	Alexander C. Morris (Chris) Freedom of Information Act (FOIA) Officer	(202) 586-3159 Alexander.morris@hq.doe.gov
Local Privacy Act Officer	Ilir Angjeli	(202) 586 3282 Ilir.Angjeli@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ilir Angjeli MA ISSO	(202) 586 3282 Ilir.Angjeli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Alexander C. Morris (Chris) Freedom of Information Act (FOIA) Officer	(202) 586-3159 Alexander.morris@hq.doe.gov
Purpose of Information System or IT Project	The primary purpose of FOIAXpress is to serve as a tool to manage, control, and determine the status of Freedom of Information Act (FOIA) and Privacy Act requests; produce statistical reports; and to serve as a data source for management information. This information may include personal information in an identifiable form from members of the public. The system automates the FOIA and Privacy Act business processes for all FOIA and Privacy Act requests received at DOE offices. FOIAXpress may also receive PII that is contained in responsive documents for both FOIA and PA requests. In each case, DOE program and legal reviewers will examine the responsive material for appropriate redactions. In the case of FOIA, sensitive PII is almost always redacted before release. For requests under the Privacy Act, sensitive PII about the requestor may be released, but PII about third parties is generally redacted. To comply with the Office of Management and Budget (OMB) M-19-10, *Guidance for Achieving Interoperability with the National FOIA Portal (NFP) on FOIA.gov,* which states that agencies with automated case management systems are required to achieve full interoperability with the Department of Justices (DOJ) NFP by accepting requests through a structured Application Programming Interface (API), the DOE FOIAXpress has integrated with the NFP using the Public Access Link (PAL). PAL is a tool that is used to integrate DOE's FOIAXpress with the DOJ's NFP. The NFP allows for requesters to submit FOIA requests electronically and the PAL API interoperability allows these NFP requests to be submitted directly into DOE's instance of FOIAXpress. DOE is examining additional features for PAL that will eventually allow the public to submit FOIA and Privacy Act requests directly into DOE FOIAXpress. FOIAXpress provides an electronic document management system that ensures that FOIA and Privacy Act requests are addressed in a timely manner. The system provides DOE with the tool that promotes the streamlining of procedures to process FOIA and Privacy Act requests by: 1) Tracking and managing FOIA and PA cases throughout the entire Department using one software application which can capture data including requester name, action office, due date, estimated completion date, disposition of case, exemptions used, costs associated; 2) Providing options for notifying requesters of request status via electronic means; 3) Providing daily, monthly, and annual reports of related activities at all sites; 4) Tracking the processing status at each stage; 5) Facilitating overall management and insight for the Chief FOIA Officer; 6) Linking Headquarters and all field sites under one system accessible from the user desktops;	

MODULE I – PRIVACY NEEDS ASSESSMENT

	7) Providing a secure environment to safeguard information; and 8) Facilitating online redaction of documents.
Type of Information Collected or Maintained by the System:	☒ SSN [may be collected for processing Privacy Act requests and included on documents responsive to FOIA or Privacy Act Requests] ☒ Medical & Health Information ☒ Financial Information ☒ Clearance Information ☐ Biometric Information ☐ 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 data, and including any other personal information that is linked or linkable to a specific individual.*	PII exists on the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

MODULE I – PRIVACY NEEDS ASSESSMENT

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

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.; • Freedom of Information Act, 5 U.S.C. 552; • Privacy Act, 5 U.S.C. 552a.

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)?**	In FOIAXpress, there are two potential sources of PII. The first is requested from the requestor: • For FOIA requests, this will typically include contact information like name, address, email, phone number and other identifying details; and • For Privacy Act requests, the requestor may also be asked to furnish their SSN in addition to their contact information. In cases where an SSN is requested, that PII will be used to verify the identity of the requestor to locate responsive records. In addition, any responsive documents containing sensitive PII, such as SSNs are safeguarded throughout the process. All PII submitted as part of a request is stored in the FOIAXpress system and access to such PII is limited to personnel in job functions relevant to the FOIA and Privacy Act processes. In addition, legal counsel would redact any PII contained in responsive documents unless that PII pertains to the individual making the request for records. Information submitted by the public to DOE to process their FOIA and PA cases is provided voluntarily. Should individuals decline to provide this information, DOE may not be able to process requests for responsive records if we do not have the necessary identifiable information.
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. Contractors are involved in the design, development, and maintenance of the system. Personal information from FOIAXpress 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, FOIAXpress, an 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.5, *Security and Privacy Controls for Information Systems and Organizations* controls and ensures the application is compliant with Federal and DOE policies. FOIAXpress 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. FOIAXpress 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.
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 will be retrieved using the individual's name or request control number generated by the FOIAXpress system.

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*.**	DOE-55 "Freedom of Information and Privacy Act (FOIA/PA) Requests for Records." Federal Register Vol. 74, No. 6/Friday, January 9, 2009. page 1059-1061.
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?	PII is obtained from the individual submitting a request or an authorized third party submitting a request on behalf of an individual.
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. Data elements are described in the DOE FOIAXpress Configuration Management Plan.
DATA USE	
11. How will the PII be used?	The information will be used to identify information maintained by DOE about individuals making FOIA and Privacy Act requests and to respond to those requests.

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. Information is not shared with other agencies. Information will be shared only with appropriate authorized users of the system from the DOE Headquarters and DOE site offices.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	There are no reports that are produced about individuals. The system produces statistical reports that do not identify 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?	No, the system does not have the capability to identify, locate, or monitor individuals beyond the limited information relating to addresses contained in the system.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	FOIAXpress 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. FOIAXpress 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.5, *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.	FOIAXpress does not verify the accuracy or completeness of the data relating to the general public. PII submitted for a FOIA or Privacy Act requests should be provided by the individual themselves or a third party authorized by the individual. The FOIA and Privacy Act process operates on the presumption that individuals are providing accurate information necessary to process their FOIA or Privacy Act request.
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 and DOE site offices. The system is hosted at DOE Headquarters by the DOE Office of the Chief Information Officer (OCIO).
RECORDS MANAGEMENT	
22. Identify the record(s).	Records include FOIA and PA requests and responses.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	□ Scheduled GRS 14, 21 a(1) and GRS 14, 11, (3)(a)(b)
24. Records Contact	Alexander C. Morris, Alexander.Morris@hq.doe.gov, 202 586-3159

MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and administrative controls are in place to prevent misuse of data by individuals with authorized 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 System Security Plan. Each user must also sign a Rules of Behavior (ROB) document that explains the system's rules of behavior and consequences for violating the rules, prior to gaining access to the system. These signed ROBs are maintained by the System Manager. The system also provides system audit logs to monitor access and user activity in the system. FOIAXpress 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. FOIAXpress 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.5, *Security and Privacy Controls for Information Systems and Organizations* controls and ensures the application is compliant with Federal and DOE policies.
26. Who will have access to PII data?	Authorized DOE federal and contractor personnel with FOIA and Privacy Act responsibilities will have access to the data in the system. Access to personal data in the system is strictly controlled based on job responsibility and function.
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 controls lists. User accounts are reviewed every six months to identify and remove users who have left the organization or whose duties no longer require access to the system.

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 System Owner is responsible for assuring proper use of data.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Alexander C. Morris** **(Print Name)** Alexander C. Morris Digitally signed by Alexander C. Morris Date: 2021.10.01 13:07:15 -04'00' **(Signature)**	
Local Privacy Act Officer	**Ilir Angjeli** **(Print Name)** Ilir Angjeli Digitally signed by Ilir Angjeli Date: 2021.10.01 13:04:08 -04'00' **(Signature)**	
Chief Privacy Officer	**William Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2021.10.01 10:00:25 -04'00' **(Signature)**	