U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: FDonline
Bureau/Office: Office of the Solicitor
Date: October 18, 2018
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

FDonline is an automated financial disclosure reporting system. It is a Software as a Service (SaaS) solution offered by Intelliworx and is used by the Department of the Interior (DOI) to automate the annual financial disclosure process required by Federal employees and other individuals to fulfill their obligations and requirements under the Ethics in Government Act of

1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified. FDonline facilitates the automation of the United States Office of Government Ethics (OGE) Form 450 and Form 278e, and helps the Departmental Ethics Office within the Office of the Solicitor at DOI ensure compliance with Federal conflict of interest laws, and regulations and requirements to preserve and promote the integrity of public officials and institutions.

FDonline maintains information from year to year so only updates to information are necessary from filers, electronically notifies filers of the annual requirement to file and guides the filer through the entire form filling process. The application automatically reminds filers of their need to file as due dates approach, allows for electronic filing, and automates management reports of non-filers. FDonline also allows the Ethics Office to review and certify the OGE Form 450 or OGE Form 278e electronically.

C. What is the legal authority?

5 U.S.C. 7301, 7351, 7353; 5 U.S.C. App. (Ethics in Government Act of 1978); 31 U.S.C. 1353; E.O. 12674 (as modified by E.O. 12731); Executive Order 12674 (as modified by Executive Order 12731); 5 CFR Part 2634, Subpart I, of the Office of Government Ethics regulations; 5 C.F.R. Part 3501--Supplemental Standards of Ethical Conduct for Employees of the Department of the Interior; and 43 CFR Part 20--Office of the Secretary of the Interior, Employee Responsibilities and Conduct

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☒ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000947

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	N/A	N/A	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

This system is covered by the following Government-wide system of records notices:

OGE/GOVT-1: Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, 68 FR 3099 (January 22, 2003), correction published at 68 FR 24744 (May 8, 2003), correction published at 77 FR 45353 (July 31, 2012), and correction published at 78 FR 73863 (December 9, 2013): https://www.gpo.gov/fdsys/pkg/FR-2003-01-22/html/03-1101.htm

OGE/GOVT-2: Executive Branch Confidential Financial Disclosure Reports, 68 FR 3101 (January 22, 2003), correction published at 68 FR 24722 (May 08, 2003): https://www.gpo.gov/fdsys/pkg/FR-2003-01-22/html/03-1101.htm

DOI also published a system of records notice for financial interest statements, DOI-03 Financial Interest Statements and Ethics Counselor Decisions, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-1999-04-14/pdf/99-9280.pdf. This notice is under review in accordance with the Privacy Act and OMB Circular A-108 and will be revised or retired as necessary consistent with the OGE government-wide SORNs and the needs of the Department.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

OGE Form 450: Executive Branch Confidential Financial Disclosure Report, OMB Control Number: 3209-0006, expires 03/21/2020.

OGE Form 278e: Executive Branch Personnel Public Financial Disclosure Report, OMB Control No: 3209-0001, expires 01/31/2021.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Group Affiliation
☒ Marital Status
☒ Spouse Information
☒ Financial Information
☒ Personal Email Address
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Other: *Specify the PII collected.*

Work grade/title, work phone, type of filer (public or confidential - OGE 278e, 450 or optional form 450-A, which is a short form for OGE 450 when there are no changes to report), types and amounts of non-federal salaries, investments, and assets, who holds the asset or investment (no identifying information about spouse or child), creditors – names and addresses, names of other employers, and name of Congressional committee considering a nominee if the filer is a Presidential nominee. Personal email address or telephone number is only collected for OGE Form 278 filers who are not at DOI at the time they file the disclosure--this includes filers who file termination reports after leaving government service. The filer will be able to access FDonline by using personal email address.

Records in this system maintained under the OGE government-wide SORNs may contain information or supporting documents including: financial information such as salary, dividends, retirement benefits, interests in property, deposits in a bank and other financial institutions; information on gifts received; information on certain liabilities; information about positions as an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, company, firm, partnership, or other business, non-profit organization, labor organization, or educational institution; information about non-Government employment agreements, such as leaves of absence to accept Federal service, continuation of payments by a non-Federal employer; and information about assets placed in trust pending disposal.

The system may also include other documents developed or information and material received in administering the Ethics of Government Act of 1978 or the Ethics Reform Act of 1989, as amended, including, ethics agreements, documentation of waivers issued to an officer or employee by an agency pursuant to section 208(b)(1) or section 208(b)(3) of title 18, U.S.C.; certificates of divestiture issued by the President or by the Director of OGE pursuant to section 502 of the Ethics Reform Act of 1989; information necessary for the rendering of ethics counseling, advice or formal advisory opinions, or the resolution of complaints; the actual opinions issued; and records of referrals and consultations regarding current and former employees who are or have been the subject of conflicts of interest or standards of conduct inquiries or determinations, or employees who are alleged to have violated department, agency or Federal ethics statutes, rules, regulations or Executive orders. These records or information

may be related to personal and family financial and other business interests, positions held outside the Government and acceptance of gifts and may include correspondence, documents or material concerning an individual's conduct, reports of investigations with related exhibits, statements, affidavits or other records obtained during an inquiry. The system may also contain reports of action taken by the agency, decisions and reports on legal or disciplinary action resulting from any referred administrative action or prosecution. OGE government-wide SORNs may be viewed at https://www.doi.gov/privacy/sorn.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems:
☒ Other: *Describe*

Information is primarily collected from individuals through the website, however, information or supporting documents may also be collected during interviews or follow up activities through email or paper or other medium.

D. What is the intended use of the PII collected?

The information collected is used to facilitate the annual financial disclosure process pursuant to the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified. The Office of Government Ethics requires certain employees to file financial disclosure reports to avoid involvement in a real or apparent conflict of interest. The purpose of this report (form) is to assist employees and agencies in avoiding conflicts of interest between their official duties and their private financial interests or affiliations. The information provided will only be used for legitimate purposes, and will not be disclosed to any requesting person unless authorized by law.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Individual employees (filers) have access only to their own forms in the system. Certain Departmental Ethics Office (DEO) senior ethics officials have the ability to view all OGE Forms 450 and OGE Forms 278e within FDonline. Other DEO ethics officials only have the ability to view the forms that have been assigned to them. Bureau Deputy Ethics Counselors see all forms submitted by their bureau employees (filers) – they do not see other Bureau forms or the DEO forms. These forms are used only for review by DOI ethics officials, to determine compliance with applicable Federal conflict of interest laws and regulations. FDonline does not conduct information sharing.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Reports may be shared with the Office of Inspector General.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

If an employee who files an OGE Form 450 or OGE Form 278e transfers to another Federal agency into another position that requires the filing of the OGE Form 450 or OGE Form 278e, the employee and/or new Federal agency may request a copy of the OGE Form 450 or OGE Form 278e that was submitted by the filer. Information may be shared with the Office of Government Ethics to perform their oversight functions, the U.S. Government Accountability Office for accounting and oversight purposes, the Department of Justice in connection to litigation related to ethics matters, and with other agencies and organizations as authorized and consistent with the routine uses published in the applicable Government-wide OGE/GOVT-1 and OGE/GOVT-2 system of records notices.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

FDonline system data may be shared with Intelliworx for system operation and maintenance purposes. Information may be shared with contractors under contract to DOI to provide support for maintenance of the system, audits, or other authorized purpose.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.* The OGE Form 278e is a publicly available document. A member of the general public may request a copy of the OGE Form 278e by using OGE 201 Form: Request to Inspect or Receive Copies of Executive Branch Personnel Public Financial Disclosure Reports or Other Covered Records. An ethics official has 30 days to comply with an OGE 201.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals may decline to complete the financial disclosure forms or provide the required information. However, there are penalties for Federal employees and other consequences for individuals who do not complete their financial disclosure reports or otherwise meet the requirements under the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics, which require the reporting of this information. Failure to provide the requested information may result in separation or disciplinary action. Filers are made aware of financial disclosure filing requirements as part of the recruitment process via statements in vacancy announcements. Filers are further notified during in-processing briefings by their Human Resources department representatives.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is provided on Form OGE 278 and Form OGE 450. Filers are made aware of financial disclosure filing requirements as part of the recruitment process via statements in vacancy announcements. Filers are further notified during in-processing briefings by their Human Resources representatives.

OGE Form 450 Privacy Act Statement:

Title I of the Ethics in Government Act of 1978 (5 U.S.C. app. 101), Executive Order 12674 (as modified by Executive Order 12731), and 5 CFR Part 2634, Subpart I, of the Office of Government Ethics (OGE) regulations require the reporting of this information. Failure to provide the requested information may result in separation or disciplinary action. The primary use of the information on this form is for review by Government officials of your agency, to determine compliance with applicable Federal conflict of interest laws and regulations. Additional disclosures may be made pursuant to the routine uses set forth in OGE/GOVT-2: (1) to a Federal, State, or local law enforcement agency if the disclosing agency becomes aware of a violation or potential violation of law or regulation; (2) to a court or party in a court or Federal administrative proceeding when the Government is a party or in order to comply with a judge-issued subpoena; (3) to a source when necessary to obtain information relevant to a conflict of interest investigation or decision; (4) to the National Archives and Records Administration in records management inspections; (5) to the Office of Management and Budget during legislative coordination on private relief legislation; (6) to the Department of Justice or in certain legal proceedings when OGE, an employee of OGE, or the United States is a party to litigation or has

an interest in the litigation and the use of such records is deemed relevant and necessary to the litigation; (7) to reviewing officials in a new office, department or agency when an employee transfers from one covered position to another; (8) to a Member of Congress or a congressional office in response to an inquiry made on behalf of an individual who is the subject of the record; and (9) to contractors and other non-Government employees working for the Federal Government to accomplish a function related to this OGE Government-wide system of records. Note: When an agency is requested to furnish such records to OGE, such a disclosure is to be considered as made to those officers and employees of the agency which co-maintains the records who have a need for the records in the performance of their official duties in accordance with the Ethics in Government Act and other pertinent authority conferred on OGE, pursuant to the provisions of the Privacy Act at 5 U.S.C. 552a(b)(1). This confidential report will not be disclosed to any requesting person unless authorized by law. See also the OGE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports Privacy Act system of records.

OGE Form 278e
Privacy Act Statement Title I of the Ethics in Government Act of 1978, as amended (the Act), 5 U.S.C. app. § 101 et seq., as amended by the Stop Trading on Congressional Knowledge Act of 2012 (Pub. L. 112-105) (STOCK Act), and 5 C.F.R. Part 2634 of the U. S. Office of Government Ethics regulations require the reporting of this information. The primary use of the information on this report is for review by Government officials to determine compliance with applicable Federal laws and regulations. This report may also be disclosed upon request to any requesting person in accordance with sections 105 and 402(b)(1) of the Act or as otherwise authorized by law. You may inspect applications for public access of your own form upon request. Additional disclosures of the information on this report may be made: (1) to any requesting person, subject to the limitation contained in section 208(d)(1) of title 18, any determination granting an exemption pursuant to sections 208(b)(1) and 208(b)(3) of title 18; (2) to a Federal, State, or local law enforcement agency if the disclosing agency becomes aware of violations or potential violations of law or regulation; (3) to another Federal agency, court or party in a court or Federal administrative proceeding when the Government is a party or in order to comply with a judge-issued subpoena; (4) to a source when necessary to obtain information relevant to a conflict of interest investigation or determination; (5) to the National Archives and Records Administration or the General Services Administration in records management inspections; (6) to the Office of Management and Budget during legislative coordination on private relief legislation; (7) to the Department of Justice or in certain legal proceedings when the disclosing agency, an employee of the disclosing agency, or the United States is a party to litigation or has an interest in the litigation and the use of such records is deemed relevant and necessary to the litigation; (8) to reviewing officials in a new office, department or agency when an employee transfers or is detailed from one covered position to another; (9) to a Member of Congress or a congressional office in response to an inquiry made on behalf of an individual who is the subject of the record; (10) to contractors and other non-Government employees working on a contract, service or assignment for the Federal Government when necessary to accomplish a function related to an OGE Government-wide system of records; and (11) on the OGE Website and to any person, department or agency, any written ethics agreement filed with OGE by an individual nominated by the President to a position requiring Senate confirmation. See also the OGE/GOVT-1 executive branch-wide Privacy Act system of records.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this PIA and the published OGE/GOVT-1: Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records, and OGE/GOVT-2: Executive Branch Confidential Financial Disclosure Reports system of records notices.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

The employees (filers) are able to retrieve their forms by email address and a password established by the filer. DOI ethics officials have access to the forms in FDonline through their user accounts, which include their email address and password. Ethics officials log into FDonline to view, certify or retrieve forms by specific employee or filer name, and can also retrieve records by form type (OGE Form 450 or OGE Form 278e).

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

FDonline allows ethics officials to view and certify OGE Form 450 and OGE Form 278e on individual filers. These forms are used by ethics officials to determine compliance with applicable Federal conflict of interest laws and regulations. The ethics official may generate a report within FDonline that shows employees who have filed their OGE forms and those employees who have not filed their forms. Reports may include a list of names and work email addresses or personal email addresses for employees who leave the agency and still need to file a financial disclosure report. This list is used by ethics officials to ensure compliance with Federal requirements; however, it may be shared with employees' supervisors in order to get the employees to file the required forms. Comprehensive reports may also be generated in FDonline to list all filers that include names and email addresses. There are no reports that pull, extract, or compile sensitive or financial information from the actual OGE Form 450 or OGE Form 278e submitted by individuals.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data is collected through forms from individual filers and is verified by ethics officials through oversight procedures established by the Office of Government Ethics to ensure compliance with

the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics, which require the reporting of this information. Any discrepancy or information found about the filer is shared with the filer to verify accuracy of the additional information.

B. How will data be checked for completeness?

It is the individual filer's responsibility to ensure the information provided in their financial disclosure reports is complete and accurate. FDonline includes required fields functionality to ensure employees complete all fields required for OGE Form 450 and OGE Form 278e. Thereafter, ethics officials review the form for completeness and make further inquiries of the filer if needed.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

It is the individual filer's responsibility to ensure the information provided in their financial disclosure reports is updated and remains current. The information in FDonline is kept current through mandatory annual updates by the employees, and some filers may be required to submit an updated financial disclosure report within 30 days of a change as required under the STOCK Act. OGE regulations require certain federal employees to file an OGE Form 450 or OGE form 278e, and these employees submit updated forms annually as long as the employees remain in a filing position.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

DOI Ethics program records are currently included under the National Archives and Records Administration (NARA)'s General Records Schedule (GRS) 2.8: Employee Ethics Records. This schedule outlines records retention for general ethics program records, referrals and notifications of conflict of interest/other violations, reports of payments, questionnaire records, ethics program reviews, ethics agreements, and financial disclosure records.

NARA sets records retention of 1 year, 3 years, and 6 years for various categories of records under this schedule.

General ethics program records for the coordination and management of agency ethics programs must be destroyed 6 years following the closure of the document/completion of the purpose for which it was created (e.g., conclusion of ethics regulatory review, making determination regarding outside employment, etc.). This authority is cited as GRS 2.8 010, DAA-GRS-2016-0006-0001.

Financial disclosure reports range between public reports (2.8 060, 061, 062, and 063), confidential financial disclosure reports (2.8 070, 071, and 072), alternative/additional financial disclosure reports (2.8 080, 081), and supporting documentation (2.8 090).

- For officials not confirmed by the U.S. Senate, in all cases, the records must be destroyed 1 year after the nominee ceases to be under consideration.
- For periodic transaction reports (OGE 278-T), records must be destroyed 7 years after receipt by the agency, or when the related Form 278 is ready for destruction.
- Requests to inspect or receive copies of executive branch personnel public disclosure reports or other records must be destroyed when the requested report is destroyed.
- All other financial disclosure reports are destroyed 6 years after receipt of the OGE form by the agency.

The GRS provides specific authorities that can be cited for all categories of records. Please see: https://www.archives.gov/files/records-mgmt/grs/grs02-8.pdf

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The OGE Form 450 and OGE Form 278 remains in the system for a period of six (6) years, then are purged or destroyed, in accordance with an approved records retention schedule and as directed by OGE regulations unless the Ethics Official is notified by the Office of Inspector General that the individual is under investigation and to keep the report until the investigation is complete. FDonline system user activity and event logs are configured to automatically overwrite the oldest activity and event once the activity or event storage capacity is reached. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to the privacy of individuals due to the large amounts of PII collected, used and maintained in the FDonline system. FDonline is hosted in the AWS GovCloud. Intelliworx is a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. Access controls and audit logs will be reviewed regularly as part of the FedRAMP continuous monitoring process. The use of DOI information systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and National Institute of Standards and Technology (NIST) guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information, and is responsible for preventing unauthorized access to the system and protecting the data contained within the system. FDonline stores all data in a secure database and access is allowed only via the application (which has its own authentication) or to an Intelliworx database administrator. FDonline has met DOI's information system security requirements, including operational and risk management policies.

FDonline is undergoing a formal Assessment and Authorization in accordance with FISMA and NIST standards. FDonline is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk that individuals may not have notice of the purposes for collecting their information, including how it will be used. Individual filers are notified of the privacy practices through this privacy impact assessment, published Government-wide OGE/GOVT-1 and OGE/GOVT-2 SORNs, detailed Privacy Act Statements on the OGE forms, and disclosures during the onboarding process.

There is a risk DOI Ethics officials may use the information in FDonline system for purposes other than those for which it was originally collected. The DOI Ethics Office approves the officials requesting access to restricted FDonline folders to those who have a valid need-to-know and monitors permissions on an ongoing basis. Hard copy documents containing PII are secured in a locked office, desk drawer or file cabinets. Also, all DOI Ethics officials and supervisors who review these documents are required to take security and privacy training and keep filers' personal information strictly confidential.

There is a risk of unauthorized access to information stored in the system. The FDonline system grants access to the system based on least privilege principle, role-based approach for user account authorization and access enforcement. Privileged account holders supporting FDonline are reviewed, authorized and approved by the System Owner. System users access the system via a secure Hypertext Transfer Protocol Secure (HTTPS) connection. Access to the FDonline system is dependent on users' roles and responsibilities, and all users are required to take annual DOI security, privacy, and records management training and also sign a DOI Rules of Behavior Agreement in order to access the system. FDonline system data is encrypted during transmission and at rest then stored within a secured database with restricted access. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users.

There is a risk of over-collection of sensitive PII / financial information from filers. The amount of financial data requested from individuals is required so Departmental Ethics Officials can thoroughly review reports for possible conflicts between official duties and private financial interest or affiliations to ensure compliance with the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics, which require the reporting of this information.

There is a risk that erroneous information concerning filers may be stored in the FDonline system. In an effort to increase accuracy, information is collected directly from filers during the hiring and on-boarding process, as well as submission of financial disclosure forms. It is the individual filer's responsibility to ensure the information they provide in their financial disclosure reports is accurate and current. Per OGE regulations filers' financial disclosure reports shall be taken at "face value" as correct, unless there is a "patent omission or ambiguity or the official has independent knowledge of matters outside of the report." A filer may initiate

an amendment to report, a reviewer may make the amendment directly, either based on additional information from the filer or independent knowledge.

There is a risk that PII information may be retained for longer than necessary. In regards to information handling and retention procedures, DOI ensures that Intelliworx is in compliance with the DOI records retention schedule approved by the National Archives and Records Administration (NARA), General Records Schedule (GRS) 2.8: Employee Ethics Records. Records Schedule. Information collected and stored within FDonline is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes

FDonline is a solution for automating the annual financial disclosure process. FDonline facilitates the automation of the United States Office of Government Ethics (OGE) Form 450 and Form 278e.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. FDonline does not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☒ Other: *Describe*

The FDonline system grants access to the system based on least privilege principle, role-based approach for user account authorization and access enforcement. Privilege account holders supporting FDonline are reviewed, authorized and approved by the System Owner. FDonline stores all data in a secure database and access is allowed only via the application (which has its own authentication) or to an Intelliworx database administrator. System users access the system via an HTTPS connection. FDonline is located within a secure hosting environment of the AWS GovCloud with controls, protections, and restricted access according to FedRAMP standards. Roles within FDonline system are identified below:

FDonline application users (filers) have access to file specified financial application disclosure forms.

DOI Ethics Administrators have access to logging into FDonline to create the appropriate filing task for a given user, then the filer is notified that they have a filing task to complete. The DOI Ethic Administrator and filer's manager are notified of the completion of this task and have the ability to log in to the system and approve the filing or perform various administrative tasks.

FDonline System Administrators, including DOI contractors supporting the system, have access to add and remove filers and modify application configurations.

Intelliworx Infrastructure Administrators have access to system infrastructure to perform system updates and patches, install and configure software, maintain database, perform backups. Intelliworx Application Administrators can add, remove application users, administer application configurations, and troubleshoot application issues. Also, Intelliworx Security Administrators

have access to perform vulnerability scans to ensure system integrity. Intelliworx Developers have read-only access on a case-by-case basis.

Users with one of the following security classifications; application administrator, infrastructure administrator, or security administrator run full device encryption on any laptop or workstation that access the Intelliworx infrastructure or application administration interface.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

FDonline system access is based on the least privilege principle, role-based approach for user account authorization and access enforcement. Privilege account holders supporting FDonline are reviewed, authorized and approved by the System Owner.

If an employee enters a filing position, they are provided access while they are in that position to complete and view their annual forms. Filer access is restricted to only their own information. Supervisors are provided access based on their supervisory relationship to employees who are filers in order to review filer information and assist in the determination of compliance with applicable Federal conflict of interest laws and regulations. Supervisor access is restricted to only information about filers that they supervise.

Agency ethics officials are provided access based on their job duties of administering the agency's financial disclosure system and determining compliance with applicable Federal conflict of interest laws and regulations. At the department level, ethics officials may have access to all information in the system. Ethics officials at lower levels have access restricted to the filers within their organization.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act contract clauses are included in contracts. In addition, access to information by contractors is restricted and controlled in accordance with FedRAMP standards.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*
☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The FDonline system collects PII as part of monitoring user activity within the system including successful and unsuccessful logon events, account management activities, object accessed such as files or folders, record any change to user rights are audited to detect suspicious activity and to support support forensic activities to investigate suspected security incidents.

Data associated with the system monitoring include: user's email performing the action; date and time; and the target of the action, if applicable. In-application auditing data remains within the application database and is subject to the same protections such as encryption as regular application data. FDonline audit and accountability policies and procedures are reviewed every two years per DOI Office of the Secretary Program and during significant system changes.

M. What controls will be used to prevent unauthorized monitoring?

Only FDonline system administrators can monitor users activity and requires proper authorization by System Owner. Additionally, infrastructure logs related to privileged functions, administrator activity, authentication and authorization checks, permission changes, data changes and deletions are automatically monitored and analyzed to detect suspicious activity and indicators of inappropriate or unusual activity. Audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

FDonline audit and accountability policies and procedures are reviewed every two years and during significant system changes. Users must consent to DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy Awareness and Records Management training, and any required role-based training before being granted access to the DOI network or any DOI system, and annually thereafter.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks

☒ Identification Badges
☐ Safes
☒ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The FDonline Information System Owner within the Office of the Solicitor is the official responsible for oversight and management of the security and privacy controls of data processed and stored by the system. The FDonline Information System Owner is the Privacy Act System Manager responsible for addressing Privacy Act rights, requests or complaints and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies in consultation with DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The FDOnline Information System Owner is responsible for the daily operational oversight and management of the FDOnline security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that access to the data has been granted in a secure and auditable manner. The FDOnline Information System Owner, Information System Security Officer, and the program officials within the Office of the Solicitor, Office of Ethics authorized to access the system are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, and appropriate DOI officials, including the Departmental Privacy Officer, in accordance with Federal policy and established DOI procedures.

Intelliworx is also responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information where such loss, compromise, unauthorized disclosure, or unauthorized access occurred at the Intelliworx controlled system areas or users to DOI. As a cloud service provider, Intelliworx must develop and maintain an incident response guide, which was approved by the DOI authorizing official at time of authorization. Intelliworx must also follow the incident response and reporting guidance contained in the *FedRAMP Incident Communications Procedure*. Intelliworx is responsible for notifying DOI officials, US-CERT, and FedRAMP of an incident, as necessary, and for working with FDonline leveraging agencies to coordinate response activities.