# Justice Management Division

**Privacy Impact Assessment**
for
Financial Disclosure Online (FDonline)

Issued by:

John M. Thompson

Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: March 11, 2026

## Section 1: Executive Summary

***Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)***

Federal ethics laws require that each agency collect information to determine the risk for conflicts of interests from employees serving in covered positions. Financial Disclosure Online (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 Justice to automate the annual financial disclosure process required by Federal employees and special government employees to fulfill their obligations and requirements under the Ethics in Government Act. FDonline facilitates the automation of the U.S. Office of Government Ethics (OGE) Form 450 and helps the Departmental Ethics Office (DEO) ensure compliance with Federal conflict of interest laws, and regulations and requirements to preserve and promote the integrity of public officials and institutions. This system allows ethics officials to review and analyze reports for potential conflicts, provide ethics guidance, and ensure compliance with ethics laws and statutes.

## Section 2: Purpose and Use of the Information Technology

***2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.***

The Ethics in Government Act of 1978, as amended (the "Act"), requires high-level Federal officials to make public disclosures of selected personal financial interests and affiliations. Section 13109 of the Act and Section 201(d) of Executive Order 12674 (as modified by E.O. 12731) provide authority for OGE to establish a confidential financial disclosure system for those executive branch employees who, though not subject to the public financial disclosure system, have duties that involve a heightened risk of potential or actual conflicts of interest. The implementing regulations for the confidential financial disclosure system can be found at 5 C.F.R. part 2634, subpart I.

The FDonline system enables the collection and review of information regarding employees' financial holdings, outside positions, and gifts received.

Information may be collected on the employee's spouse and dependent children,

including financial holdings and employment information. Information may also be collected on individual creditors, gift-providers, and employers, including name and city/state.

The U.S. Department of Justice requires a system or tool to replace the current manual process for filling out, filing, tracking, mailing, and document retention/destruction of the OGE Form 450 for new entrants or current employees who are required to file. The system will capture the same information electronically that is currently captured in the paper-based process for OGE Form 450. The system shall also automate the process related to filing, tracking, mailing, and document retention/destruction. The system shall also support the following:

- Multi-user support with custom roles
- Document retention/destruction for OGE 450
- Digitized OGE Form 450
- Workflow management
- Assigning/unassigning tasks in a workflow
- Notification reminders
- Data collection and reporting

Intelliworx shall provide 24 hours, 7 days a week online accessibility and filing services to OGE Form 450 confidential financial disclosure filers.

Since 2018, FDonline and the underlying Intelliworx platform have been FedRAMP authorized. Each year, Intelliworx pays for a FedRAMP-approved third party assessment organization (3PAO) to conduct a FedRAMP aligned system security review and testing. The resulting report and supporting documentation are made available to all agency information system security officers (ISSOs) through our FedRAMP-managed document repository. This allows individual agencies to access system security documents and avoid the significant costs entailed by individual, redundant system assessments.

In addition, FDonline has a continuous monitoring (ConMon) process since becoming FedRAMP authorized. The process involves agencies registering their Authority to Operate (ATO) letters with the FedRAMP Program Management Office (PMO) to maintain access to our system security documentation. Intelliworx provides status reports to the agency ISSOs and facilitate discussions with them to ensure all are aware of current system security status, have an opportunity to ask questions of Intelliworx and their agency colleagues, and make suggestions to improve system security.

### *2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

| Authority | Citation/Reference |
|---|---|

| | |
|---|---|
| Statute | 5 USC § 7301, 7353, App. (Ethics in Government Act of 1978); 31 USC § 1353 |
| Executive Order | Executive Order 12674 (as modified by E.O. 12731) |
| Federal regulation | Executive Branch Financial Disclosure 5 C.F.R. part 2634 |
| Agreement, memorandum of understanding, or other documented arrangement | |
| Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A, B, C, D | First name, last name of employees, assets, potential individual creditors, sources of outside gifts, and outside employers |
| **Date of birth or age** | | | |
| **Place of birth** | | | |
| **Sex** | | | |
| **Race, ethnicity, or citizenship** | | | |
| **Religion** | | | |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | | | |
| **Tax Identification Number (TIN)** | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Driver's license** | | | |
| **Alien registration number** | | | |
| **Passport number** | | | |
| **Mother's maiden name** | | | |
| **Vehicle identifiers** | | | |
| **Personal mailing address** | | | |
| **Personal e-mail address** | | | |
| **Personal phone number** | | | |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account information** | X | A, B, C, D | Retirement investments with financial institutions, assets and income for user, spouse, and dependent children (names are not used for spouse or children) |
| **Applicant information** | | | |
| **Education records** | | | |
| **Military status or other information** | | | |
| **Employment status, history, or similar information** | X | A, B, C, D | Agency and outside employment information including employer name, type, and position for employees |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | | | |
| **Certificates** | | | |
| **Legal documents** | | | |
| **Device identifiers, e.g., mobile devices** | | | |
| **Web uniform resource locator(s)** | | | |
| **Foreign activities** | | | |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | | | |
| **Juvenile criminal records information** | | | |
| **Civil law enforcement information, e.g., allegations of civil law violations** | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Whistleblower, e.g., tip, complaint, or referral** | | | |
| **Grand jury information** | | | |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | | | |
| **Procurement/contracting records** | | | |
| **Proprietary or business information** | X | A, B, C, D | Work email address, agency, branch/unit, and business address, and work phone number for employees. City/state information for potential individual creditors, sources of outside gifts, and outside employers. |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |
| ***Biometric data:*** | | | |
| - **Photographs or photographic identifiers** | | | |
| - **Video containing biometric data** | | | |
| - **Fingerprints** | | | |
| - **Palm prints** | | | |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | | | |
| - **Scars, marks, tattoos** | | | |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | | | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | X | A | Logging in/out information: User ID, date/time of access. |
| - **User ID** | X | A | System admi/audit data logs User ID. |
| - **User passwords/codes** | | | |
| - **IP address** | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - **Date/time of access** | X | A | System administrator/audit data logs date/time of access. |
| - **Queries run** | | | System administrator/audit data and user ID of authorized user. |
| - **Contents of files** | | | |
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C, D | Outside work activities as pertinent to required/ confidential financial disclosures for OGE ethics forms, including positions held outside of U.S. Government, gifts/travel reimbursements, and agreements/arrangements (Requested on OGE Form 450) |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

| **Directly from the individual to whom the information pertains:** | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | | Online | X |
| Phone | | Email | | | |
| Other (specify): Applicable employees enter and/or access their own information in the FDonline system. | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | | Other Federal entities | |
| State, local, tribal | | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | | | |
| Other (specify): The information is entered by the user who is a Federal employee of DOJ. | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): The information is not from a non-government source. | | | | | |

## Section 4: Information Sharing

***4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.***

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | | | X | Reports will be reviewed and certified by ethics officials for criminal conflicts of interest to comply with ethics regulations. All users must sign-in using a PIV card and are granted access to use the system via an email invitation. Data is not shared with anyone outside of the ethics official and certifying official which is the employee's supervisor. |
| DOJ Components | | | X | Information may be shared with the Criminal Division if a violation of criminal law is discovered. |
| Federal entities | | | X | The OGE form 450 may be provided in a court case as part of a criminal prosecution. |
| State, local, tribal gov't entities | | | | |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | X | | | Information collected in FDonline may be shared and used by counsel, parties, and courts for litigation purposes through a official request through the litigation process. |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | | | | |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Other (specify): | | | | |

***4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

The confidential financial disclosure data is confidential, protected information. It is not shared with anyone other than the filer, ethics official, and certifying official, which is the employee's direct supervisor.

## Section 5: Notice, Consent, Access, and Amendment

***5.1 What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.***

The OGE Form 450 includes a Privacy Act Statement which is replicated in the system. The statement outlines the purpose and authorities for the collection of the information, the names of the relevant SORNs, the routine uses of the records as published in the SORNs, and the potential penalties for failure to provide the information.

Generalized notice is also provided by the following SORNs: 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

DOJ-002, Department of Justice Information Technology, Information System, and

Network Activity and Access Records, 86 FR 37188 (7-14-2021).

5.2 ***What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

The confidential financial disclosure filing requirement is part of the employee's official duties as a Federal employee and is a condition of employment. Therefore, if the applicable employee refuses to provide the required information in OGE Form 450, subsequent employment/disciplinary action may be initiated as a result. Disciplinary action includes suspension or removal from the position.

***What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why***. The information in the system is provided annually by applicable employees. Applicable employees may gain access to information pertaining to them by filing a Freedom of Information Act (FOIA) and/or Privacy Act request. Procedures on how to complete a FOIA/Privacy Act request are published here: Office of Information Policy | Make a FOIA Request to DOJ

## Section 6: Maintenance of Privacy and Security Controls

***6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).***

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** The ATO date is 3/31/2023 and expires in 3 years from the ATO date.<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** |

| | |
|---|---|
| | ▪ **DOJ Risk Level: Low** |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |
| X | **This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information, and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:**<br>FIPS 199 Security Categorization for Financial Disclosure Online is considered Moderate in all confidentiality, integrity, and availability. This is derived from the FedRAMP independent assessment of the Intelliworx infrastructure. Justification for the Moderate nature of FDonline is due to its record keeping of personal identities and authentication methods as well as general income information that is stored or is authorized to be stored within. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**<br>FDonline is FedRAMP certified and performs monitoring, testing and evaluation in accordance with FedRAMP controls. The last 3PAO assessment was Nov. 2024. Access to the system is limited to persons who have an appropriate security clearance, which is regularly reviewed. Information is safeguarded by use of proper passwords and user identification to access the system. Only those DEO personnel who require access to perform their official duties may access the system and information in the system. |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:**<br>Intelliworx system components are configured to automatically log system and user account activity/events in accordance with system audit requirements and appropriate configuration benchmarks. Intelliworx system infrastructure activity/event logs are automatically input into the Intelliworx AlienVault Security Information and Event Management (SIEM) tool for automated monitoring and analysis to detect suspicious activity and indicators of |

| | |
|---|---|
| | inappropriate or unusual activity and alert appropriate Intelliworx Infrastructure and Security Administrators. |
| X | **Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. |
| X | **Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** There is no FDonline specific privacy-related training. New users can search for help using the online system and contact their ethics official for questions. There are user tutorials and help menu options to learn how to use the system and enter data. |

***6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

FDonline is an Intelliworx SaaS FedRAMP-certified system which has no direct interconnections with any other system. Security controls are monitored on an ongoing basis. Role-based, least privilege access, and two-factor authentication are used for access to the system. Individuals are only granted access to the functionalities within the system necessary to accomplish their assigned tasks and responsibilities. Access and authorization requests are documented, authorized, and approved by the individual's manager prior to account creation. Intelliworx system infrastructure activity/event logs are routinely monitored and analyzed by Intelliworx Infrastructure and Security Administrators to detect suspicious activity and indicators of inappropriate or unusual activity. Application security logs are available for review by Intelliworx Security Officers.

The Intelliworx Cloud platform is a software application platform that allows customer agencies to streamline and automate workflows in any number of mission areas.

Software modules built on the Intelliworx Cloud platform allows users to:

- Define the people who are part of a given business workflow: assigning them roles, permissions, tasks, and responsibilities.
- Gather information critical to the workflow in a streamlined and intuitive way.
- Define the tasks that need to be completed by users and provide mechanisms for approvals, notifications/reminders, and reporting.

- Integrate with existing government systems to accept, process and store data.
- Map gathered data to official government forms.

The Intelliworx platform is also a suite of tools that allows customized solutions called *modules*.

*At the code level,* the Intelliworx platform is a common set of code libraries that allow for the creation of software "modules" that perform specific process automation functions based upon customer requirements.

*At an application level,* Intelliworx modules appear as independent web applications with unique URLs and separate logins for each web application. Customers are given access to only the URL and login appropriate for the module(s) they are using.

*At the infrastructure level,* the Intelliworx Cloud is an environment hosted and secured at AWS GovCloud. Multiple Intelliworx modules are hosted in this environment but are completely segregated except when an integration is authorized between two modules. The only services shared by these modules are the security systems that oversee them.

***6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.***

Record retention falls under General Records Schedule 1.1, Item 010. It is subject to Disposition Authority DAA-GRS-2013-0003-0001, and standard record retention is six years.

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

_____ No. ___X_ Yes.

***7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

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

DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (7-14-2021).

## Section 8: Privacy Risks and Mitigation

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.***

***Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:***

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules).***

  DOJ is required to collect and maintain the information required by the confidential financial disclosure report such as outside sources of income, liabilities, outside positions and gifts and travel reimbursements. This information is required to be collected and maintained for 6 years to ensure the integrity of the Department and its programs. This data is protected within the FDonline system which requires a PIV card to sign in. The user must log in using a PIV card and update information which will be saved in the FDonline system. DEO will ensure that this confidential information will not be comprised by unauthorized users. DEO updates the system and removes filers as users when they leave the Department. Former employees cannot access the system since they will no longer have a PIV card.

- ***Sources of the information*** The information is from the user who is required to file the confidential financial disclosure report. The information collected can be changed by the user and the user must update their report annually and edit any information that changed. The information collected is only what is required by Federal law and statute outlined in section 2.1. The information is certified by the user's supervisor who will certify that

there are no conflicts with the user's Federal position. An ethics official within DEO will certify the report.

- ***Type of technology employed (e.g. AI/ML),***
- ***Specific uses or sharing*** FDonline is used to collect and maintain information from a user who has been identified as a confidential financial disclosure filer. Confidential financial disclosure reports are required to avoid potential or apparent conflicts of interest for the employee's position. The information collected includes non-Federal assets and income, liabilities, outside positions, gifts and travel reimbursements for the employee, their spouse and dependent children.

- ***Privacy notices to individuals, and The privacy statement is listed on the first page of the confidential financial disclosure report.***
  DOJ employees are provided with a Privacy Act Statement as described in section 5.1 5 U.S.C. § 13109, Executive Order 12674 (as modified by Executive Order 12731), and 5 CFR Part 2634, Subpart I, of the Office of Government Ethics (OGE) 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 source when necessary to obtain information relevant to a conflict of interest investigation or decision; (3) to the National Archives and Records Administration in records management inspections; (4) to the Office of Management and Budget during legislative coordination on private relief legislation; (5) when the disclosing agency determines that the records are arguably relevant to a proceeding before a court, grand jury, or administrative or adjudicative body, or when the adjudicator determines the records to be relevant to the proceeding; (6) to reviewing officials in a new office, department or agency when an employee transfers or is detailed from one covered position to another; (7) to a Member of Congress or a congressional office in response to an inquiry made on behalf of and at the request of an individual who is the subject of the record; (8) 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; (9) to appropriate agencies, entities and persons when there has been a suspected or confirmed breach of the system of records, the agency maintaining the records has determined that there is a risk of harm to individuals, the agency, the Federal Government, or national security, and the disclosure is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and (10) to another Federal agency or Federal entity, when the agency maintaining the record determines that information from this system of records is reasonably necessary to assist the recipient agency or entity

in responding to a suspected or confirmed breach or in preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity, the Federal Government, or national security.

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.

- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.*** The Departmental Ethics Office mitigates the risk of unauthorized access by ensuring the users assigned to the application are the users that are required to obtain access to the FDonline system. Users must be added into the OKTA system[1] and granted access to the FDonline application. Users have their authorization removed if they leave the Department. The Departmental Ethics Office administrator of the system updates users regularly and removes access to users that left. Accounts can also be locked so that no one can obtain access to the report and users accounts can be deactivated. There are two users that have access, the administrator and the supervisor.

  DOJ staff receive annual security awareness and cybersecurity training that includes privacy, technical and physical controls over sensitive information on an annual basis. There is a minimum risk of potential disclosure of sensitive information and staff enforces access controls and removes users from the application in OKTA. There is a tracking of user data to review then users log into the system and when communications are sent to users.

  Data transmission within and outside the system is encrypted using the transport layer security (TLS) protocol[2]. Data within the system is used and shared only when compatible with the system's authorities and required by the agency's mission in accordance with DOJ standard contract clauses DOJ-02 and DOJ-05 clauses.

[1] DOJ's use of OKTA is covered by separate privacy documentation available here: https://www.justice.gov/opcl/media/1347416/dl?inline.
[2] TLS provides privacy and data integrity between two communicating applications. For more information see: https://csrc.nist.gov/glossary/term/transport_layer_security.