Federal Bureau of Prisons

Privacy Impact Assessment
for the
FDOnline System

Issued by:
Michael Rogers
Acting Chief RIM Section /SCOP

Approved by: Michelle Ramsden
Senior Counsel
Office of Privacy & Civil Liberties
U.S. Department of Justice

Date approved: June 17, 2025

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the 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 Executive Branch agency collect information to determine the risk of conflicts of interest from employees with certain duties. For Federal Bureau of Prisons (FBOP) employees to which this requirement applies ("applicable employees"), this data is collected and reviewed by FBOP Ethics Office staff on behalf of the Office of Government Ethics (OGE). The information is collected on the OGE Form 450 and includes financial and employment information regarding the employee and connected individuals. The Ethics Office uses FDOnline, a system that enables the collection of the information required by the Form 450 from applicable employees across the FBOP.

FDOnline is a service provided by Intelliworx, a third-party vendor who manages the website, maintains the software application, and stores the data at the direction of the FBOP. Intelliworx is a FedRAMP-approved cloud service provider. The system also provides a method by which the FBOP Ethics Office may review and analyze compliance with Federal ethics laws in a uniform manner. FBOP has prepared a Privacy Impact Assessment for FDOnline because this system collects, maintains, and disseminates information in identifiable form about individuals.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, 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 FBOP Ethics Office staff input the names of employees who are required to complete an OGE Form 450 into FDOnline, and then FDOnline sends out notifications to the employees via email and subsequent email reminders if the required information is not filed within a specified time frame. Applicable employees enter required information into the FDOnline system annually in accordance with the OGE Form 450. The information collected includes financial and employment information on the applicable employee and their spouse and dependent children. Information on creditors, outside positions, and gifts are also collected. The information is reviewed by the FBOP Ethics Office within the FDOnline system, replacing the earlier practice of reviewing paper-based forms. Supervisors of applicable employees must review and verify compliance. If there are issues with the applicable employee's information, FBOP Ethics Officers contact the applicable employee directly with questions through email, phone, or in-person communications independent from the system. With the applicable employee's consent, they either correct or clarify the information within FDOnline themselves or direct the employee to do so.

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
X	Statute	5 USC § 7301, 7353, App. (Ethics in Government Act of 1978); 31 USC § 1353
X	Executive Order	E.O. 12574 and 12674 (as modified by E.O. 12731)
X	Federal Regulation	5 C.F.R. Part 2634, Subpart I of the Office of Government Ethics regulation; 5 C.F.R. Part 3501
	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, and D	Names of applicable employees, and potential individual creditors, gift-providers, and employers.
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity or citizenship			
Religion			

(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
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
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, and D	Assets, liabilities, financial interests, loan information, gifts, and travel reimbursements of applicable employees, spouses, and dependent children.
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	Agency and outside employment information including employer name, type and position of applicable employees, spouses, and dependent children.
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: 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
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			
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:			
- **User ID**	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- **User passwords/codes**	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- **IP address**	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- **Date/time of access**	X	A	System admin / audit data and User ID of authorized FBOP personnel.
- **Queries run**	X	A	System admin / audit data and User ID of authorized FBOP personnel.

(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
- **Content of files accessed/reviewed**			
- **Contents of files**	X	A	System admin / audit data and User ID of authorized FBOP personnel.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Work e-mail address, agency, branch/unit, and business address, and work phone number of applicable employees. City/state information of potential individual creditors, gift providers, and employers. Outside work activities as pertinent to required/confidential financial disclosures for OGE ethics forms, including positions held outside of the 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	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): Applicable employees enter their own information into FDOnline, however, if there are issues with an applicable employee's information, FBOP Ethics Officers may contact the employee with questions through email, phone, or in-person communications and either correct or clarify the information within FDOnline themselves or direct the employee to do so.					

Government sources:					
Within the Component		Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			

Government sources:
Other (specify):

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information (routine uses mentioned in applicable SORN(s), if not the primary intended sharing, need not be mentioned here) 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	Applicable FBOP employees enter information in the FDOnline system. Data in the system is accessed and reviewed by FBOP Ethics staff. Supervisors of applicable employees must review and verify compliance.
DOJ Components				
Federal entities			X	OGE employees may be provided read-only access to perform program reviews of the FBOP Ethics Program.
State, local, tribal gov't entities				
Public				

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.**
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, witnesses, and courts or other judicial tribunals for litigation purposes; however, such sharing and use would only be shared when appropriate requests for records are requested through the litigation process.
Private sector				
Foreign governments				
Foreign entities				
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.

N/A

Section 5: Notice, Consent, Access, and Amendment

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

Public notice is provided via the applicable SORNs:

- OGE/GOVT-1, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, 89 Fed. Reg. 17470 (Mar. 11, 2024), available at: https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-%201+SORN+(2024)
- OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports, 84 Fed. Reg. 47301 (Sep. 9, 2019), available at: https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-2+SORN+(2019).

The OGE Form 450 also 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.

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.

Federal ethics laws require the collection of the information to determine risks for conflicts of interest from applicable employees with certain duties. 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.

5.3 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 on the FBOP's website at www.bop.gov.

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):** An ATO was approved for the FBOP Financial Disclosure System (FDOnline) on June 4, 2024 and will expire on June 3, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:** No relevant outstanding POAMs.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** 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 FBOP 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:** User and system administration activities are regularly audited to ensure staff roles are current. Access controls are implemented in FDOnline and are audited yearly. User access is authorized by the FBOP Ethics Office.
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**.
	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: No FDOnline-specific privacy-related training is provided. However, new ethics staff review OGE training videos that may include privacy-related components.

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.

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.)

DAA-GRS-2014-0005-0012 – Confidential financial disclosure reports – All other reports. To be retained temporarily. Destroy 6 years after receipt of the OGE Form 450 by the agency, or when no longer needed for active investigation, whichever is later.

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, 89 Fed. Reg. 17470 (Mar. 11, 2024), available at: https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-%201+SORN+(2024)
- OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports, 84 Fed. Reg. 47301 (Sep. 9, 2019), available at: https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-2+SORN+(2019).

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?

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),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Risks Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish FBOP's official duties is a potential threat to privacy arising from FDOnline. Additional risks to

privacy are inherent when the personal data is particularly sensitive or if the information is not maintained securely. For example, FBOP collects and maintains sensitive information on applicable employees and connected individuals within FDOnline, such as financial and employment information, which is used to determine risks of conflicts of interest from those employees.

The unnecessary collection of data poses a risk of the loss of personal information for the applicable employees. FBOP mitigates this risk by only collecting and retaining the data that is required to fulfill Federal ethics requirements, namely the information in OGE Form 450.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, the information is collected directly from the applicable employees on an annual basis to ensure that the information is up-to-date and accurate. The information provided by the applicable employee is reviewed by their supervisors to ensure compliance and by the FBOP Ethics Office, as part of the Office of General Counsel (OGC), who analyze the information provided.

Collected information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include encryption at rest and in transit, and the required use of proper passwords and user identification codes to access the system.

b. Potential Risks Related to the Use of Information

Potential threats to privacy arising from FBOP's use of the information in FDOnline include the risk of unauthorized access to information, and threats to the integrity of the information arising from unauthorized access or improper disposal of information.

FBOP mitigates this risk through the implementation of data access controls, ensuring information is provided only to those individuals who require access to perform their official duties. Access to the system is limited to those persons who have an appropriate security clearance, which is regularly reviewed, and a need to know based on job function.

FBOP staff are provided information security awareness training with regards to privacy, information security, and technical and physical controls over sensitive information on an annual basis. When a FBOP employee departs from the FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user's access to the FDOnline system.

c. Potential Risks Related to the Dissemination of Information

There is a privacy risk to individuals arising from the potential disclosure of sensitive information to persons not authorized to receive it and from unauthorized data modification and misuse. This risk is mitigated by enforcing access controls and encryption (as described above) and by providing auditing of user and system administration activities. Data transmission, both within and outside the system, is encrypted using the TLS protocol. 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-02 and DOJ-05 clauses.