Version Number: 01-2015

U.S. Department of Commerce
National Technical Information Service

Privacy Impact Assessment
for the
Financial Disclosure Online (FDonline)

Reviewed by: Heather Lynch, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.08.04 17:51:26 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NTIS/FDonline

Unique Project Identifier: 27000

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

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 278. FDonline helps employees fulfill their obligations and help make the process of filling out forms hassle-free. It saves the information from year to year so only updates to information are necessary. FD Online electronically notifies filers of the requirement to file and provides a link to a program that walks 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.

The information collected by the system includes: full name, home address, email address, agency with address, grade/title, work phone, type of filer (public or confidential- OGE278 or 450), types and amounts of salaries, investments, and assets, who holds the asset or investment (no personal 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.

FDonline stores all data, even PDFs in an Oracle database and allows access to said database only via the application (which has its own authentication) or an NTIS database administrator. System users access the system via an HTTPS connection. FDonline is located within a secure government data center with restricted access. NIST SP 800-53 Rev 4 Moderate controls are in place for the system. Data at rest is encrypted using FIPS 140-2 approved measures.

(b) a description of a typical transaction conducted on the system

FDonline transactions include the following operations: an ethics administrator for an agency creates a filing for an OGE-450 or 278 filer. The filer is given a login to enter the system and complete the filing. Once the filer has completed entry of all the required information, PDF versions of the required documents are rendered. The ethics administrator then has the ability to review, approve or request additional information from the filer. Once the Review of the filing is complete, the filing remains in the system for a period of six (6) years, then purged, as directed by OGE regulations.

(c) any information sharing conducted by the system

FDonline does not conduct information sharing.

(d) a citation of the legal authority to collect PII and/or BII

Title I of the Ethics in Government Act of 1978 (5 U.S.C. App.), Executive Order 12674 (as modified by Executive Order 12731), and 5 CFR Part 2634, Subpart I, of the Office of Government Ethics regulations require the reporting of this information.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The FIPS 199 security impact categorization for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
_X_ This is an existing information system that has not undergone any changes that create new privacy risks.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)* (Note: This is an existing system that has not undergone any changes.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	X

d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	X	For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	

For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information in FDonline is used only for review by Government officials of the federal employee's agency, to determine compliance with applicable Federal conflict of interest laws and regulations.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.oge.gov/Web/OGE.nsf/Resources/Privacy+and+Security?OpenDocument	
X	Yes, notice is provided by other means.	Specify how: Notice provided on Form 278 and Form 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 department representatives.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Filers are notified during in-processing briefings by their Human Resources department representatives of their option to decline to provide PII. Declining to provide PII effectively declines employment. The filing information is required for employment. If an individual declines to provide the information they may be subject to disciplinary action by their employing agency or other authority. Penalties are outlined in 5 CFR Part 2634, Subpart G.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Filers are notified during in-processing briefings by their Human Resources department representatives of the uses of their PII. The filing information is required for employment. If an individual declines to provide the information they may be subject to disciplinary action by their employing agency or other authority. Penalties are outlined in 5 CFR Part 2634, Subpart G.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Forms 278 and 450 are filed/updated annually. Individuals wishing to inquire whether this system of records contains information about them should contact, as appropriate: a. For records filed directly with OGE by non-OGE employees, contact the OGE Deputy Director, Office of Agency Programs, Office of Government Ethics, Suite 500, 1201 New York Avenue, NW., Washington, DC 20005–3917; b. For records filed with a Designated Agency Ethics Official (DAEO) or the head of a department or agency, contact the DAEO at the department or agency concerned; and c. For records filed with the FEC by candidates for President or Vice President, contact the FEC General Counsel, Federal Election Commission, 999 E Street, NW. Washington, DC 20463. Individuals wishing to request access to their records should contact the Designated Agency Ethics Official or designee at the agency where the reports were filed. Individuals must furnish the following information for their records to be located and identified: a. Full name. b. Department or agency and component with which employed or proposed to be employed. c. Dates of employment. d. Reasonably specify the record content being sought. Individuals requesting access must also follow OGE's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 2606).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.

X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/10/15 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

FDonline stores all data, even PDFs in an Oracle database and allows access to said database only via the application (which has its own authentication) or an NTIS database administrator. System users access the system via an HTTPS connection. FDonline is located within a secure government data center with restricted access.

NIST SP 800-53 Rev 4 Moderate controls are in place for the system. Data at rest is encrypted using FIPS 140-2 approved measures.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: OGE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports Privacy Act system of records notice.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NARA General Records Schedule 25
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Contains enough PII to identify an individual. Name, home address, email, job title, work address, financial information, and salary.
X	Quantity of PII	Provide explanation: Contains PII for several thousand users. Used by 19 different government entities.
X	Data Field Sensitivity	Provide explanation: Private financial information.

	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.