

U.S. Securities and Exchange Commission

Confidential Financial Disclosure System (CFDS)

PRIVACY IMPACT ASSESSMENT (PIA)



February 1, 2022

Office of Ethics Counsel

Privacy Impact Assessment

Confidential Financial Disclosure System

Section 1: System Overview

1.1 Name of Project or System

Confidential Financial Disclosure System (CFDS)

1.2 Is the system internally or externally hosted?

- Internally Hosted (SEC) SEC Office of Information Technology (OIT)
- Externally Hosted
(Contractor or other agency/organization)

1.3 Reason for completing PIA

- New project or system
- This is an existing system undergoing an update
- First developed:
Last updated:
Description of update:

1.4 Does the system or program employ any of the following technologies?

- Enterprise Data Warehouse (EDW)
- Social Media
- Mobile Application (or GPS)
- Cloud Computing Services
- Web Portal
- None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

Federal agencies are required to ensure the confidence of citizens in the integrity of the government by detecting potential or actual conflicts of interest through the collection of Form 450 from certain employees. The United States Office of Government Ethics (OGE) designates certain government positions as "covered filing positions." The SEC Office of the Ethics Counsel (OEC) uses Confidential Financial Disclosure System (CFDS), an internally hosted encrypted SharePoint site, to collect, review, certify, track, and maintain OGE Form 450 Financial Disclosure Reports. SEC employees in covered positions are required to use annually CDFS to complete Form 450 for financial disclosure. Employees may be required to provide statements and amended statements of personal and family holdings and other interests in property; income; gifts and reimbursements; liabilities; agreements and arrangements; outside positions; and other information related to conflict of interest determinations. After employee information is entered into CFDS by the employee, it is reviewed and certified by OEC personnel and the Administrative Officer (AO) in the employee's office or division. CFDS auto generates a unique link to a Form 450 for each employee in a covered filing position.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Title I of the Ethics in Government Act of 1978 (5 U.S.C. App), Executive Order 12674 (as modified by Executive Order 12731); 5 CFR. Part 2634, subpart I, of the Office of Government Ethics regulations concerning Confidential Financial Disclosure Reporting; and SEC Supplemental Ethics Regulations, 5 CFR. Part 4401

Privacy Impact Assessment

Confidential Financial Disclosure System

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

- No
 - Yes
- If yes, provide the purpose of collection:
- If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

- No
 - Yes, a SORN is in progress
 - Yes, there is an existing SORN
- [OGE/GOVT-2](#) *Executive Branch Confidential Financial Disclosure Reports*

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

- No
- Yes, OMB No. 3209-0006, Expires 11/30/21

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The privacy risk related to the purpose of the collection include personal information is collected without a clear purpose or without clear legal authority. This risk is mitigated by collecting information as authorized and in accordance with the collection purpose identified in SORN [OGE/GOVT-2](#) *Executive Branch Confidential Financial Disclosure Reports*.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

- The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

- | | | |
|---|--|---|
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Alien Registration | <input type="checkbox"/> Financial Accounts |
| <input type="checkbox"/> Taxpayer ID | <input type="checkbox"/> Driver's License Number | <input type="checkbox"/> Financial Transactions |
| <input type="checkbox"/> Employee ID | <input type="checkbox"/> Passport Information | <input type="checkbox"/> Vehicle Identifiers |
| <input type="checkbox"/> File/Case ID | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Employer ID |
| <input type="checkbox"/> Other: | | |

General Personal Data

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Marriage Records |
| <input type="checkbox"/> Maiden Name | <input type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Financial Information |
| <input checked="" type="checkbox"/> Alias | <input type="checkbox"/> Home Address | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Telephone Number | <input type="checkbox"/> Military Service |
| <input type="checkbox"/> Age | <input type="checkbox"/> Email Address | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Education Records | <input type="checkbox"/> Health Plan Numbers |
| <input type="checkbox"/> Civil or Criminal History | <input type="checkbox"/> Zip Code | |
| <input checked="" type="checkbox"/> Other: Positions held outside the SEC; Agreements or arrangements outside the SEC | | |

Work-Related Data

- | | | |
|--|--|---------------------------------|
| <input checked="" type="checkbox"/> Occupation | <input checked="" type="checkbox"/> Telephone Number | <input type="checkbox"/> Salary |
|--|--|---------------------------------|

Privacy Impact Assessment

Confidential Financial Disclosure System

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Job Title | <input checked="" type="checkbox"/> Email Address | <input type="checkbox"/> Work History |
| <input checked="" type="checkbox"/> Work Address | <input type="checkbox"/> Certificate/License Number | <input type="checkbox"/> Business Associates |
| <input type="checkbox"/> PIV Card Information | <input type="checkbox"/> Fax Number | |
| <input checked="" type="checkbox"/> Other: Employee Division/Office | | |

Distinguishing Features/Biometrics

- | | | |
|--|---|--|
| <input type="checkbox"/> Fingerprints | <input type="checkbox"/> Photographs | <input type="checkbox"/> Genetic Information |
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature |
| <input type="checkbox"/> Other: | | |

System Administration/Audit Data

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> User ID | <input checked="" type="checkbox"/> Date/Time of Access | <input type="checkbox"/> ID Files Accessed |
| <input type="checkbox"/> IP Address | <input type="checkbox"/> Queries Ran | <input type="checkbox"/> Contents of Files |
| <input type="checkbox"/> Other: | | |

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

PII is collected, used, shared, and maintained in CFDS to facilitate the submission of Form 450 to OGE and to assist in reviewing for completeness, actual and potential conflicts of interest, and other ethics issues, and to track the status of Form 450 submissions and certifications in and from offices and divisions.

3.3 Whose information may be collected, used, shared, or maintained by the system?

- SEC Employees
 Purpose: Form 450 collects certain information required by ethics regulations from those employees who hold positions designated as Form 450 filer positions.
- SEC Federal Contractors
 Purpose:
- Interns
 Purpose:
- Members of the Public
 Purpose:
- Employee Family Members
 Purpose: Form 450 collects certain information about the financial interests of the filer's spouse and dependent children.
- Former Employees
 Purpose: OEC maintains Form 450s after employees depart the SEC, as required by the records retention schedule required by OGE and approved by the Office of Records Management Services (ORMS).
- Job Applicants
 Purpose:
- Vendors
 Purpose:
- Other:
 Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

Privacy Impact Assessment

Confidential Financial Disclosure System

The SEC collects only a limited amount of personal information required for form completion. No PII is used for testing, training, or research.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

No.

Yes.

Disposition authority number DAA-GRS-2014-0005-0011. [GRS 2.8](#) *Employee Ethics Records*, item 071, *Confidential Financial Disclosure Reports*, requires retention of Form 450 records for six years.

3.6 What are the procedures for identification and disposition at the end of the retention period?

At the end of each retention period, OEC seeks permission from the Office of Records Management Services to destroy applicable records (more than six years old). Once permission is granted, OEC properly disposes of records from that calendar year.

3.7 Will the system monitor members of the public, employees, and/or contractors?

N/A

Members of the Public

Purpose:

Employees

Purpose:

Contractors

Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The identified privacy risk is that filers may report more personal financial information than is required and that such information may be inappropriately accessed by unauthorized parties. OEC mitigates this risk by using an electronic version of the Form 450 that limits the information provided to that required under regulation. Unauthorized access is mitigated through encrypting both data in-transit and at-rest. Role-based controls are in place to restrict access to the Form 450 data authorized roles.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

Privacy Act Statement

Appears on [Form 450](#) that filers digitally sign in the application.

System of Records Notice

SORN OGE/GOVT-2 *Executive Branch Confidential Financial Disclosure Reports*

Privacy Impact Assessment

Date of Last Update:

Web Privacy Policy

Privacy Impact Assessment

Confidential Financial Disclosure System

- Other notice:
User Guide and training materials for Reviewers, and User Guide for AOs are posted on the OEC's SharePoint site.
- Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The potential identified privacy risk is inadequate notice. This risk is minimal and mitigated by providing privacy notice and Privacy Act Statements on the Form 450 in CFDS. 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. In addition, this PIA and SORN OGE/GOVT-2 *Executive Branch Confidential Financial Disclosure Reports* provide notice to individuals about the purpose for information collection and how information is used.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

OEC reviews and analyzes the information on the Form 450 and may ask reviewers and filers questions related to the information presented, may send the Form 450 back to the filer for correction or amendment, may send the Form 450 back to the reviewers to analyze and comment on a potential ethics issue, and may provide ethics advice and guidance to the filers and reviewers.

5.2 Will internal organizations have access to the data?

- No
- Yes

Organizations: OEC has access to all filer information and contents of all Form 450s. AOs have access to filer information for the filers working in offices under their management and authority but do not have access to the content of the Form 450s. Reviewers in those offices have access to both filer information and to the content of the Form 450s but only for filers assigned to them for review. Data in the system also may be shared with all SEC divisions and offices internal organizations.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

The potential identified privacy risk is inappropriate disclosure of personal information to unauthorized individuals. This risk is mitigated by implementing access controls in CFDS to restrict access to information on Form 450 to authorized users based on their assigned work duties.

5.4 Will external organizations have access to the data?

- No
- Yes

Organizations: OEC may disclose information within CFDS to organizations external to OEC consistent with the disclosures authorized in Privacy Act 5 U.S.C. 552a(b) or with the routine uses listed in SORN OGE/GOVT-2.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

Privacy Impact Assessment

Confidential Financial Disclosure System

The potential risk of inadvertent disclosure is heightened when non-Federal entities are involved. Once information is received by an external organization that is not a Federal government entity (e.g., State and local law enforcement), the disclosure risk may increase. This privacy risk is mitigated, as State and local sharing is extremely rare and additional risk mitigating measures are in place. Email transmitted to external organizations (e.g. DOJ in connection with a legal proceeding) from SEC is encrypted.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

- Directly from the individual.
- Other source(s):

6.2 What methods will be used to collect the data?

Data in the Form 450 is entered directly by the user. OEC program managers and AOs enter other data in CFDS (e.g., filer name; reviewer name).

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

Individuals are responsible for ensuring that the information entered is accurate and complete. OEC Reviewers ensure that information provided by individuals on Form 450 is complete or that the filer responded “No” for the reporting statement on the cover page. The OEC review consists of a manual examination of information to identify conflict of interest, inadequate disclosure, or other data entry errors.

6.4 Does the project or system process, or access, PII in any other SEC system?

- No
- Yes.

System(s): CFDS accesses user IDs from Active Directory (AD) and stores them in a master user information list within CFDS for access control. CFDS also pulls the following data from Enterprise Human Capital Repository (EHCR) system: User ID, Extended Leave, Account Status, Enrollment ID, and Last Update Date. This information is used to create a list of personnel who can access the site.

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

The potential risk is the collection and use of inaccurate or incomplete data. To mitigate this risk, OEC staff review information collected in Form 450 submitted by employees. If it is determined that information is inaccurate or questionable, OEC staff contacts employees to ensure data quality and integrity.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Form 450 is mandatory for “covered positions” and filing of a financial disclosure report is a condition of employment as mandated by statute. Individuals do not have the right to consent to particular uses of the information.

Privacy Impact Assessment

Confidential Financial Disclosure System

7.2 What procedures are in place to allow individuals to access their information?

Individual filers may view but not amend data already entered on a submitted Form 450, unless the Form 450 is returned by a reviewer or by OEC. Filers may contact the reviewer(s) of their Form 450 if their Form 450 is still pending review. If their Form 450 has already been received by OEC, they may also contact OEC to request their Form 450s be returned for correction, amendment, or annotation.

7.3 Can individuals amend information about themselves in the system? If so, how?

Individuals can view their information going back six years and are able to amend/correct inaccurate information. The filer contacts the OEC Program Manager (PM) to ask that their certified record be amended. If warranted, the PM can revert the form status back to Pending Amendment, which then ushers the Form 450 back through the certification process within the respective Division or Office.

7.4 Discuss the privacy risks related to individual participation and redress. How were these risks mitigated?

The risks associated with participation and redress are low to non-existence. Because the filers are the source of the information, the assumption is that the information is accurate. The filer has a duty to provide accurate information and the freedom to update this information whenever it becomes necessary. Only the filers or authorized individuals will be able to access or make corrections/changes to their information.

Section 8: Security

8.1 Can the system be accessed outside of a connected SEC network?

No

Yes

If yes, is secured authentication required?

No

Yes

Not Applicable

Is the session encrypted?

No

Yes

Not Applicable

8.2 Does the project or system involve an online collection of personal data?

No

Yes

Public URL:

8.3 Does the site have a posted privacy notice?

No

Yes

N/A

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC staff and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security-related responsibilities and how to fulfill them.

9.2 Does the system generate reports that contain information on individuals?

Privacy Impact Assessment

Confidential Financial Disclosure System

- No
- Yes

CFDS uses the Microsoft Power BI application to run reports derived from data in the system (e.g., filers overdue on an annual Form 450 filing requirement). This information may contain filer name and other filer information (e.g., grade, office).

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

- No
- Yes
- This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

- No
- Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Residual risk related to access is minimal because user authentication is implemented using PIV synched with AD and role based access control is implemented.

Privacy Impact Assessment

Confidential Financial Disclosure System

Approval

Signature/Date

David Bottom

Chief Information Officer

Director, Office of Information Technology

Senior Agency Official for Privacy