

## 1. Contact Information

**A/GIS/IPS Director**

Bureau of Administration

Global Information Services

Office of Information Programs and Services

## 2. System Information

(a) Name of system: Financial Disclosure Management System

(b) Bureau: L/EX

(c) System acronym: FDM

(d) iMatrix Asset ID Number:

(e) Reason for performing PIA:

New system

Significant modification to an existing system

To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

## 3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?  
\_\_\_ Yes \_\_\_ No

(b) What is the security Assessment and Authorization (A&A) status of the system?

FDM received an Authorization to Operate (ATO) under the DoD Information Assurance Certification and Accreditation Process (DIACAP) on December 9, 2013.

(c) Describe the purpose of the system:

FDM was developed by the Army to provide electronic filing, review, and management of a filer's reportable information on the Office of Government Ethics (OGE) Form 278, Public Financial Disclosure Report, and OGE Form 450, Confidential Financial Disclosure Report. The Department of State, through a contract with the Army, uses FDM to provide for the secure filing and review of information reported as required by the financial disclosure regulation (5 C.F.R. Part 2634) of the OGE. FDM stores the reportable information for review by appropriate agency officials.

(d) Describe the PII that the system collects, uses, maintains, or disseminates:

The system collects and maintains information reportable pursuant to 5 C.F.R. Part 2634, including information about personal and family investments, interests in property, salary, retirement benefits, and cash accounts; information about gifts received; information about certain liabilities; information about non-federal positions and employment; information about non-federal employment agreements; and other information related to conflict of interest determinations. The system also stores related documents uploaded as attachments, such as a filer's position description and Ethics Agreement.

- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?

5 U.S.C. 7301, 7351, 7353; 5 U.S.C. App. (Ethics in Government Act of 1978), as amended; E.O. 12674 (as modified by E.O. 12731); 5 C.F.R. Part 2634.

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes  If yes, provide:

- SORN Name and Number: OGE/GOVT-1; OGE/GOVT-2
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 31, 2012

No  If a SORN is not required, explain how the information is retrieved without a personal identifier.

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes  No

If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes  No

(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov).)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): NARA General Records Schedule 25
- Type of information retained in the system: Filer's reported information.
- Length of time the information is retained in the system: For filers who do not end up taking the position for which they are under consideration, the information will be destroyed 1 year after nominee or candidate ceases to be under consideration for the position, except that documents needed in an ongoing investigation will be retained until no longer needed in the investigation. For all other filers, the information will be destroyed after 6 years, except that documents needed in an ongoing investigation will be retained until no longer needed in the investigation.

**4. Characterization of the Information**

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other:

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary? N/A  
Yes \_\_\_\_ No \_\_\_\_

- If yes, under what authorization?

(c) How is the information collected?

FDM is a secure, web-based application. Disclosure report filers follow a step-by-step report wizard process to prepare and submit (eSign) the disclosure report form and to attach any necessary/supporting documentation. Reviewing officials may supplement reported information upon review when necessary to elaborate or clarify a filer's report. That supplement may take the form of a comment, note, or separate document attached in FDM with that filer's report.

(d) What process is used to determine if the information is accurate?

Filers are the source of the information. By signing the form electronically, a filer certifies that the information is true, complete, and correct to the best of his or her knowledge. Once the filer has eSigned the report, reviewing and certifying authorities use FDM to process and review the disclosures.

(e) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Filers are required to update and certify the information maintained in FDM as required under 5 CFR Part 2634.

(f) Does the system use information from commercial sources? Is the information publicly available?

FDM does not use information from commercial sources. Public financial disclosure reports can be made public pursuant to 5 CFR Part 2634.

(g) Is notice provided to the individual prior to the collection of his or her information?

Yes. Filers self-report and are aware of the collection of data. The standard DoD Information System Use & Consent notice banner is presented whenever the user tries to login to FDM. At login, an FDM user is presented with a Privacy Act Statement. The FDM user clicks “OK” to proceed to login.

- (h) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes \_\_\_\_\_ No   x

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

Filing an OGE Form 278 or OGE Form 450 is a condition of employment for those employees required to file, as mandated by statute. Use of FDM to file these reports is mandatory for such Department of State employees.

- (i) How did privacy concerns influence the determination of what information would be collected by the system?

FDM collects financial disclosure information as required by the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified, and OGE and agency regulations thereunder. The system does not collect information other than for the purpose of complying with these laws.

## **5. Use of information**

- (a) The intended use(s) for the information is/are:

Ethics officials use the information filers provide via FDM to determine compliance with applicable Federal laws and regulations and to identify and resolve any potential conflicts of interests between an employee’s official duties and private financial interests and affiliations. A filer’s ethics official and filer’s initial reviewer use FDM to review and certify the information as required in order to process the disclosures.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. FDM was developed to provide secure electronic filing, review, and management of a filer’s reportable information as required by the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified, and OGE and agency regulations thereunder. Filers, ethics officials, and other authorized users make use of the information in a manner consistent with these purposes.

(c) Does the system analyze the information stored in it? Yes \_\_\_ No x

If yes:

- (1) What types of methods are used to analyze the information?
- (2) Does the analysis result in new information?
- (3) Will the new information be placed in the individual's record? Yes \_\_\_ No \_\_\_
- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?  
Yes \_\_\_ No \_\_\_

**6. Sharing of Information**

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

A financial disclosure report is shared internally with those agency users who have an official need to know the report contents for administration of the Department's financial disclosure program. A report filer and appropriate Department reviewing and ethics officials (e.g., initial reviewer, certifying ethics officials) may view a filer's financial disclosure report.

OGE Form 278 Public Financial Disclosure Reports may be released to the public after a proper request on OGE Form 201 (Request to Inspect or Receive Copies of OGE Form 278/SF-278 or Other Covered Records), as required by law.

Where necessary to accomplish an agency function and compatible with the purpose for which the information was collected, the information may also be disclosed to other Bureaus within the Department of State, the Department of Justice or another Federal Agency, to a court, and to parties in litigation.

(b) What information will be shared?

Information contained in the filer's OGE Form 278 financial disclosure reports may be shared with a member of the public when requested through OGE Form 201.

Where necessary to accomplish an agency function and compatible with the purpose for which the information was collected, information on FDM may also be disclosed to other

Bureaus within the Department of State, the Department of Justice or another Federal Agency, to a court, and to parties in litigation.

(c) The purpose for sharing the information is:

The reports are shared internally as required to assure compliance with governing regulatory procedures and to preserve and promote the integrity of public officials.

Public financial disclosure reports are public, and upon receipt of procedurally sufficient requests from members of the public, the Department must release the public financial disclosure report to the requestor.

Information on FDM may be disclosed to other Bureaus in the Department, the Department of Justice or another Federal agency, to a court, and to parties in litigation only where necessary to accomplish an agency function and compatible with the purpose for which the information was collected.

(d) The information to be shared is transmitted or disclosed by what methods?

A report filer and appropriate Department reviewing and ethics officials (e.g., initial reviewer, certifying ethics officials) may view a filer's financial disclosure report on FDM.

In other circumstances, once a requestor's identification and need to know is verified, the information is transmitted in printed form delivered via courier, fax, email, or regular mail. Requestors may also visit the office for personal pick up.

(e) What safeguards are in place for each internal or external sharing arrangement?

Policies and procedures are in place to limit the use of and access to all data in FDM. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards that include restricting access to authorized personnel who have a need to know.

Information on FDM is shared internally with those agency users who have an official need to know the report contents.

All requests from the public for the OGE Form 278 Public Financial Disclosure Report must be on the OGE Form 201. Information is shared externally with the public only to the extent required by law, pursuant to a request submitted in accordance with the proper procedures using OGE Form 201. Pursuant to 5 C.F.R. Section 2634.603 (c), each agency shall within thirty days after any public report is received by the agency, permit

inspection of the report by or furnish a copy of the report to any person who makes written application as provided by agency procedure.

Information shared with other Bureaus in the Department of State, Federal agencies, courts, or parties in litigation is provided on a case by case basis and is not directly accessible by agencies outside the Department of State environment.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The main privacy concern associated with internal and external information sharing is unauthorized access to the personal information shared. These concerns are addressed through the safeguards identified in section 6(e).

## **7. Redress and Notification**

- (a) What procedures allow individuals to gain access to their information?

FDM users are registered before access is allowed. A Department FDM administrator assigns a user one or more “roles” (with data access privilege) during registration. Role assignment/data access is limited to only the data/information needed to perform the user’s assigned duties. Filers or their appointed representatives will have unlimited access to their information.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information? Yes   x   No

If yes, explain the procedures.

If a filer submits information on FDM and realizes an error has been made, the filer or his designated representative may access the system and make any necessary corrections. If the filer provided incorrect information in already-certified reports, the filer may add comments noting the corrections.

If no, explain why not.

- (c) By what means are individuals notified of the procedures to correct their information?

Filers may consult with Department ethics officials concerning any corrections to their information, as well as the FDM help desk for technical assistance. This PIA also

provides notice concerning corrections, as described above. In addition, users receive instructions on the use of the system, including the process for correcting information.

## **8. Security Controls**

- (a) How is the information in the system secured?

FDM is a secure, web-based application. Access to the system is limited to specifically authorized personnel, such as filers or their personally appointed representatives, initial reviewers, and ethics officials. Security features include user authentication, AES 256-bit encryption, and network and physical security protection. The system's servers are housed in a secure Department of Defense facility.

- (b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

A Department FDM administrator assigns a user one or more "roles" (with corresponding data access privilege) during registration. FDM users must be registered for specific roles. Access to reported information is role-based. The data resides on a server to which only IT staff and support personnel have access; the users access the data only through the FDM application. Personal and financial information collected is presumptively protected and treated as private and sensitive in nature with access limited to select individuals/roles related to a particular filer. The Defense Information Systems Agency (DISA) vets the credentials of IT personnel who administer the system. Application administrators are bound by Army regulation and individual non-disclosure agreements to safeguard private information from unauthorized persons. Note, however, that completed OGE Form 278 Public Financial Disclosure Reports may be released to the public after a proper request.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Servers are patched on a regular basis or as updates are provided. Hardware firewalls and Intrusion Detection Systems (IDS) monitor and block unauthorized connections outside the enclave. The servers use current anti-virus software to check for viruses in real time and check all files weekly. Patches to the system's software and servers are installed nightly. The system's audit logs make a record of every time a filer's information is changed, including when a filer's information is changed by an authorized user. Logs are checked for unauthorized access or server problems on a routine basis.

- (d) Explain the privacy training provided to authorized users of the system.

As a part of the implementation process all users will receive training on the use of the system. In addition, at login, FDM users will get a Privacy Advisory (PA). The PA details the requirements and statutory obligations for the collection of the information. Department employees are required to fulfill privacy training.

- (e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users? Yes  No   
If yes, please explain.

All communications between the FDM servers and the user's desktop/laptop computers use a 128 bit, DES approved HTTPS protocol. FDM is hosted on a server that has been hardened using current Defense Information Systems Agency (DISA) guidance. Ports and services that are not needed have been removed from the operating system.

- (f) How were the security measures above influenced by the type of information collected?

Controls are in place and effective in mitigating all risks to an acceptable level for protecting systems and data up to and including 'For Official Use Only' Privacy Act data. In addition, FDM is role-based so that only authorized users with an official need to know may access a filer's reported financial information.

## **9. Data Access**

- (a) Who has access to data in the system?

Access to the system is limited to specifically authorized personnel: filers or their personally appointed representatives, initial reviewers, and ethics officials.

- (b) Access to data in the system is determined by:

A Department FDM administrator assigns a user one or more "roles" (with corresponding data access privilege) during registration.

- (c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes  No

Procedures, controls, and responsibilities regarding access to data in the system are documented in Department of Defense regulations, policies, and guidance.

- (d) Will all users have access to all data in the system or will user access be restricted?  
Please explain.

Role assignment/data access is limited to only the data/information needed to perform the user's assigned duties.

- (e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?

FDM is a secure, web-based application. FDM users must be registered for specific roles. Access to reported information is role-based.