Privacy Impact Assessment
for the

# Financial Disclosure Management (FDM)

September 30, 2008


**Contact Point**
**Cynthia D. Morgan, Financial Disclosure Program Manager**
**Ethics Division Office of General Counsel**
**(202) 447-3514**

**Reviewing Official**
**Hugo Teufel III**
**Chief Privacy Officer**
**Department of Homeland Security**
**(703) 235-0780**

## Abstract

The Ethics Division of the Office of General Counsel (OGC) of the Department of Homeland Security (DHS) is publishing this Privacy Impact Assessment (PIA) for the Financial Disclosure Management System (FDMS). FDMS is a web-based initiative developed to provide a mechanism for individuals to complete, sign, review, and file financial disclosure reports, first required by Title I of the Ethics in Government Act of 1978. This PIA is being conducted because FDMS collects personally identifiable information.

## Overview

FDM is a secure, web-based software program, owned by the Department of the Army that helps guide financial disclosure Filers to accurately prepare and electronically file annual Executive Branch Public Financial Disclosure Reports [Standard Form (SF) 278] and Executive Branch Confidential Financial Disclosure Reports [Office of Government Ethics (OGE) Form 450]. DHS will initially use FDMS for SF 278 report Filers during fiscal year 2009. At some point DHS will request approval from the Office of Government Ethics to also use the system for OGE 450 Filers. An update to this PIA will be published for use of the FDMS to file OGE Form 450.

All FDM users (financial disclosure Filers and other authorized users) will be entered into the system and assigned their role (e.g., Filer, Supervisor, Assistant, Supervisor, legal staff for filer, and certifying official(s)) before access is allowed. A Department FDM Administrator will assign users one or more "Roles" (with corresponding data access privileges) during registration. Filers use their DHS computer system user logon and password to gain access to FDM. Upon accessing the system, Filers follow a step-by-step report wizard process to prepare and submit (eSign) the disclosure report form and to attach any necessary documentation. Once the filer has eSigned the report, FDM sends email notification(s) to the filer's servicing ethics official and the filer's supervisor for appropriate review/certification. Reviewing and certifying authorities use FDM to process the disclosures.

FDM contains information about the review status and report progress (e.g., draft, under review, complete) of the SF 278. FDM facilitates online review of the electronically filed disclosures. The disclosures are reviewed to identify and resolve potential conflict of interest issues between a Filer's reported financial interests and the Filer's official agency responsibilities.

All FDM records are maintained in accordance with the requirements of the Ethics in Government Act of 1978, the Ethics Reform Act of 1989, as amended, the Executive Order 12674 as modified, 5 CFR part 2634, and Office of Government Ethics regulations. These requirements include the filing of financial status reports, reports concerning certain agreements between the covered individual and any prior private sector employer, ethics agreements, the preservation of waivers issued to an officer or employee pursuant to Section 208 of Title 18, and certificates of divestiture issued pursuant to Section 502 of the Ethics Reform Act. Such statements and related records are required to assist employees and DHS in avoiding conflicts between duties and private financial interests or affiliations. Ethics officials are also required to maintain information being researched or prepared for referral concerning employees or former employees of the Federal Government who are the subject of complaints of misconduct or alleged violations of ethics

laws. These complaints may be referred to the Office of the Inspector General of the agency where the employee is or was employed or to the Department of Justice.

# Section 1.0 Characterization of the Information

## 1.1 What information is collected, used, disseminated, or maintained in the system?

FDMS contains the following PII: Financial information such as salary, dividends, retirement benefits, interests in property, deposits in a bank and other financial institutions; information on gifts received; information on certain financial liabilities; information about positions as an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, company, firm, partnership, or other business, non-profit organization, labor organization, or educational institution; information about non-Government employment agreements, such as leaves of absence to accept Federal service, continuation of payments by a non-Federal employer; and information about assets placed in trust pending disposal.

When information not specifically required to be reported by the disclosure report or statute is found in the Filers' records, Filers will be notified and asked to delete such information. Examples of this type of information are as follows: a rental property address, spouse/child name, and bank account numbers. This report-related PII is not mandated by statute and will not be maintained on FDMS or the DHS Ethics Office.

## 1.2 What are the sources of the information in the system?

The financial disclosure Filers, generally DHS employees, are the sources of the information in the system.

## 1.3 Why is the information being collected, used, disseminated, or maintained?

FDMS maintains the financial disclosure records 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. DHS ethics officials use this information to determine whether any potential conflicts exist between employee duties and private financial interest or affiliations, thereby preserving and promoting the integrity of public officials and institutions.

## 1.4 How is the information collected?

Information is collected via web interface and stored on secure servers for access by authorized personnel. Those who are obligated by statute to file (Filers) will prepare the report themselves or appoint representatives to enter the information on their behalf.

### 1.5 How will the information be checked for accuracy?

Because the Filers are the source of the information, the assumption is that the information is accurate. Filers will sign the forms electronically and in doing so they certify that the information is true, complete, and correct.

### 1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

All records are maintained in accordance with the requirements of 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.

### 1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a risk that the Filer will input the financial information incorrectly.

Mitigation: This potential risk is mitigated by requesting that the Filer review and verify the accuracy of the inputted information prior to electronic signature and submission.

Privacy Risk: Due to the collection method for FDMS, there exists the potential for electronic eavesdropping by unauthorized parties as Filers enter data.

Mitigation: This risk has been mitigated by the implementation of strong security protections for the web environment. Data submission via FDMS is protected using the Secure Socket Layer protocol and encryption. Additional discussion of system security protections for FDMS are discussed in Section 8.0 of this PIA.

## Section 2.0 Uses of the Information

### 2.1 Describe all the uses of information.

DHS ethics officials use the information Filers provide in SF-278 via FDMS 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. Filer's ethics official and Filer's supervisor use FDM to review and certify the information as required in order to process the disclosures.

### 2.2 What types of tools are used to analyze data and what type of data may be produced?

Financial disclosure data is stored, but not manipulated by the system.

## 2.3 If the system uses commercial or publicly available data please explain why and how it is used.

In addition to the financial data input by the Filer or their representative, Filers will be able to scan and attach documents such as brokers statements.

## 2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Individuals who have legitimate access to PII could exceed their authority and use the data for unofficial purposes.

Mitigation: FDM minimizes potential risks by implementing various security protections. FDM users are registered before access is allowed. A Department FDM administrator assigns a user one or more "roles" (with corresponding data access privilege) during registration. Role assignment/data access is limited to only the data/information needed to perform the user's assigned duties.

As mentioned in Section 1.7, data submissions are protected by use of SSL protocol to safeguard reported information. The data resides on a server to which only IT staff and support personnel have access based on their official Government duties, and the users accesses 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. Application administrators are bound by Army regulation and individual non-disclosure agreements to safeguard private information from unauthorized persons. Note, however, that completed SF 278 Public Financial Disclosure Reports, may be released to the public after a proper request.

For security purposes and to ensure that FDM remains available to only authorized users, FDM uses software programs to monitor network traffic and to identify unauthorized attempts to upload or change information, to cause damage, or to deny service to authorized users. Server logs are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. Unauthorized attempts to upload information or change information on this service are strictly prohibited.

# Section 3.0 Retention

## 3.1 What information is retained?

The following information is retained: Financial information such as salary, dividends, retirement benefits, interests in property, deposits in a bank and other financial institutions; information on gifts received; information on certain liabilities; information about positions as an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, company, firm, partnership, or other business, non-profit organization, labor organization, or educational institution; information about non-Government employment agreements, such as leaves of absence to accept Federal service, continuation of payments by a non-Federal employer; and information about assets placed in trust pending disposal.

## 3.2 How long is information retained?

In accordance with the National Archives and Records Administration General Records Schedule for ethics program records, these records are generally retained for a period of six years after filing, or for such other period of time as is provided for in that schedule for certain specified types of ethics records. In cases where records are filed by, or with respect to, a nominee for an appointment requiring confirmation by the Senate, when the nominee is not appointed or withdraws voluntarily as a nominee, the records are generally destroyed one year after the date the individual ceased being under Senate consideration for appointment. However, if any records are needed in an ongoing investigation, they will be retained until no longer needed in the investigation. Destruction is by electronic deletion.

## 3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, NARA approved the retention schedule.

## 3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a risk that PII could be maintained for a period longer than necessary to achieve agency objectives.

Mitigation: Although there is always a risk inherent in retaining personal data for any length of time, FDM data retention periods identified in the NARA schedule are consistent with the concept of retaining personal data for only as long as necessary to support the agency's mission. NARA concurred by approving the ethics program's long standing schedule.

# Section 4.0 Internal Sharing and Disclosure

## 4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

When an individual transfers to any other DHS operational component with a dedicated servicing ethics office and the individual occupies another Department position requiring financial disclosure reporting, reports pertaining to that individual will also be transferred to the servicing office. The reports are required to assure compliance with governing regulatory procedures and to preserve and promote the integrity of public officials.

## 4.2 How is the information transmitted or disclosed?

Once the 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.

## 4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: The main risk associated with internal information sharing is unauthorized access to the personal information shared.

Mitigation: DHS policies and procedures are in place to limit the use of and access to all data in FDMS. 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. A financial disclosure report is shared internally with those agency users who have an official need to know the report contents. A report Filer and appropriate Department reviewing officials (*i.e.*, supervisor, legal advisor, certifying official) associated with that filer may view a filer's financial disclosure report. In addition, senior level ethics officials may see the status of a particular filer's report progress toward certification/ approval.

# Section 5.0 External Sharing and Disclosure

## 5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Public financial disclosure reports are indeed 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. 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 the Department of Justice or other Federal Agency, to a court, and to parties in litigation. Information is provided on a case by case basis and is not directly accessible by agencies outside the DHS environment. Additionally, in that the program is owned by the Department of the Army, Army IT

personnel will have access to system data to ensure the program functions properly and are acting as contractors in this relationship; non-disclosure agreements are in place to cover this sharing.

### 5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The current SORN addressing data collection activities on which the FDM system is based is OGE – GOVT 1, 68 Federal Register (FR) 3098, dated January 22, 2003. All external sharing is covered by an appropriate routine use. All sharing is compatible with the purpose for which the information was originally requested.

### 5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

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. Reports are transmitted in printed form delivered via courier, fax, email, or regular mail. Requestors may also visit the office for personal pick up.

### 5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

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 during internal use. Completed SF 278 Public Financial Disclosure Reports may be released to the public, but only after submission of a proper request. Application administrators are bound by regulation and individual non-disclosure agreements to safeguard report-related private information found in the Filers' records not subject to release pursuant to statute in the manner of the report itself.

## Section 6.0 Notice

### 6.1 Was notice provided to the individual prior to collection of information?

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.

Filers are also provided general notice through the Government-wide Privacy Act system of records notice (SORN) issued by the Director, U.S. Office of Government Ethics (OGE), i.e., GOV OGE-1 (68 FR 3098), as well as presented with a Privacy Act statement on the initial login page.

### 6.2 Do individuals have the opportunity and/or right to decline to provide information?

Providing information on the SF 278 is a voluntary act on the part of the individual seeking employment, although the filing of a financial disclosure report is a condition of employment as mandated by statute.

### 6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to consent to particular uses of the information, but DHS' use of the information will conform to the appropriate policies of the GOV OGE-1 SORN (68 FR 3098).

### 6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Filers self report and are aware of the collection of data. At login, an FDM user is presented with a Privacy Act Statement. The FDM user clicks "OK" to proceed to login. A filer's login evidences the use consent.

When a member of the public requests a copy of a Filer's Public Financial Disclosure Report, as a courtesy, the Department servicing ethics office notifies the Filer of the request and once again informs the Filer that the report must be released per statute.

## Section 7.0 Access, Redress and Correction

### 7.1 What are the procedures that 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.

Requests for access to records in this system should be directed to Ms. Cynthia D. Morgan, Financial Disclosure Program Manager, Office of General Counsel, 245 Murray Lane, MSC 3650, Washington DC 20528-3650, 202-447-3514 (cynthia.morgan@dhs.gov).

### 7.2 What are the procedures for correcting inaccurate or erroneous information?

If a Filer submits a SF 278 via FDMS and realizes an error has been made, the Filer or his designated representative would simply access the system and make any necessary corrections.

### 7.3 How are individuals notified of the procedures for correcting their information?

The GOV OGE-1 SORN (68 FR 3098) provides Filers with guidance regarding the procedures for correcting information. This PIA also provides similar notice. In addition, as a part of the implementation process all users (Filers, their representatives, supervisors, and reviewers) will receive training on the use of the system including the process for correcting information.

### 7.4 If no formal redress is provided, what alternatives are available to the individual?

Filers are provided opportunity for redress as discussed above.

### 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

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 individuals authorized by them will be able to access or make corrections/changes to their information.

## Section 8.0 Technical Access and Security

### 8.1 What procedures are in place to determine which users may access the system and are they documented?

Access to the system will be limited to specifically authorized personnel: Filers or their personally appointed representatives, Supervisors, and Ethics Officials. Supervisors and Ethics Officials have read-only access to Filer data. Security features include user authentication, AES 256-bit encryption, and network and physical security protection, as documented in DHS Sensitive Systems Policy Directive 4330A Information Security Program, Version 6.1, September 24, 2008 (user authentication); DHS 4300A Sensitive Systems Handbook, Version 6.1, September 23, 2008; Attachment I, Workstation Logon, Logoff and Locking Procedures; Attachment L Password Management, Version 6.1, September 23, 2008; Section 5.4 Network and Telecommunications Security; DHS Management Directive MD Number: 11030.1, 4/21/2003 PHYSICAL PROTECTION OF FACILITIES AND REAL PROPERTY.

## 8.2 Will Department contractors have access to the system?

Yes, contractors support portions of the FDM environment. Contractors may access the system, upon Filer authorization, for the purposes such as data entry and processing financial disclosure reports. Access is provided to contractors only as needed to perform their duties as required in the agreement between OGE and the contractors and as limited by relevant SOPs.

## 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or 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.

## 8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Army issued an Interim Authority to Operate on July 10, 2008. They are expecting to issue ATO in November 2008.

## 8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

FDM is a secure, web-based application. FDM users must be registered for specific roles. Access to reported information is role-based. 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. Servers are patched on a regular basis or as updates are provided. Hardware firewalls and Intrusion Detection Systems (IDS) are monitoring and blocking unauthorized connections outside the enclave. The servers use current anti virus software to check for viruses in real time and check all files weekly. Virus definitions are set to automatically download nightly. Logs are checked for unauthorized access or server problems on a routine basis.

## 8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

FDM uses software programs to create summary statistics, which are used for website planning and maintenance, determining technical design specifications, and analyzing system performance. For security purposes, and to ensure that FDM remains available to all authorized users, FDM uses

software programs to monitor network traffic, to identify unauthorized attempts to upload or change information, to cause damage, or to deny service to authorized users. Server logs are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. Unauthorized attempts to upload information or change information on this service are strictly prohibited.

# Section 9.0 Technology

## 9.1 What type of project is the program or system?

FDM is a Windows 2003 server running- IIS 6.0 (SSL port 443); 2 x Windows 2003 servers running -SQL 2005 Standard cluster (DB port 1433); Windows 2003 Standard server running- Weblogic 9.2 , Infomosaic SecureXML Digital Signature & Encryption version 2.5.146.44, Java version 1.5.0_06. Ports 6090(SSL), 5090(non-SSL); Outgoing Connection to FDM application server over TCP/IP using Secure Sockets Layer (SSL). Access is required to the configured SSL port (on FDM Application server) ONLY; Incoming HTTPS (standard SSL port) connectivity from the internet.

## 9.2 What stage of development is the system in and what project development lifecycle was used?

Present life-cycle phase: Milestone C, 2 of 3 phases completed, operations & maintenance for phases 1 &2, design development for phase 3. Phase 3 anticipated to be complete mid-FY09. There are periodic releases to upgrade and enhance FDM based on new technology, new concepts, or new user requests.

## 9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

FDM minimizes potential risks by SSL to safeguard reported information. In addition, users are restricted to accessing data based on their role(s) in FDM. 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. Application administrators are bound by Army regulation and individual non-disclosure agreements to safeguard private information from unauthorized persons. Note, however, that completed SF 278 Public Financial Disclosure Reports, may be released to the public after a proper request.

For site management, FDM uses software programs to create summary statistics, which are used for website planning and maintenance, determining technical design specifications, and analyzing system performance. For security purposes, and to ensure that FDM remains available to all authorized users, FDM uses software programs to monitor network traffic, to identify unauthorized attempts to upload or change information, to cause damage, or to deny service to authorized users. Server logs are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. Unauthorized attempts to upload information or change information on this service are strictly prohibited.

# Approval Signature

Original Signed and on File with DHS Privacy Office
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security