Electronic Disclosure Information Management System (E–DIMS) – Privacy Impact Assessment

PIA Approval Date – Feb. 15, 2011

System Overview:
The Electronic Disclosure Information Management System (E–DIMS) is the IRS nation–wide management information system for inventory control, casework management, and standardized reporting for the National Disclosure Program. E–DIMS is a tool to help Disclosure Managers balance both program and casework management responsibilities. Each office must ensure timely and accurate data entry. E–DIMS contains historical notes from case workers in working Freedom of Information Act (FOIA) and Privacy Act (PA) requests as well as requests under Section 6103 of the Internal Revenue Code (IRC). The data from this system is used for disclosure staffing plans, peer reviews, congressional reporting, executive briefings, system analysis efforts, and other statistical uses affecting disclosure.

Systems of Records Notice (SORN):

- IRS 48.001--Disclosure Records
- IRS 34.037--Audit Trail and Security Records

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer data used in this system consists of tax return information, consisting of documents gathered in preparing responses to FOIA and PA requests as well as requests under Section 6103 of the Internal Revenue Code (IRC).

B. Employee data used in this system consists of Identification and Authentication (I&A) data of E–DIMS users with access to the system. E–DIMS also records employee name, User ID, office of assignment, cases assigned to the employee, time spent on cases as entered by the employee, and case activity notes entered by the employee. Recording of employee actions on cases is mandatory on E–DIMS.

C. E–DIMS uses audit trails as required by IRS 2.1.10, Information Systems Security, May 1998. A Functional Security Coordinator has been assigned. E–DIMS provides an Activity Log (audit trail) that indicates when a security violation has occurred. E–DIMS user additions, deletions, or modifications are only granted upon receipt of online5081, Automated Information System User – Registration/Change Request. The E–DIMS Project Manager determines membership to the E–DIMS user groups. E–DIMS limits user input and editing and running reports to only the cases assigned to the user or within the user's office. Expanded Display only access is available for certain cases nationally, where coordination among offices is required, for example FOIA requests and Letter Forwarding work.

D. E–DIMS also collects data regarding the identity and location of the requesting entity/organization/individual. Statistical information is collected concerning correspondence received in Disclosure offices, specifically: dates of receipt and closure, disposition of FOIA/PA cases required for reports to Congress, and time applied by other offices within the Service on those cases. Names and addresses of Federal and State agencies receiving tax information from the Service and notes concerning Safeguard Reviews conducted on those agencies are collected, as well as information concerning disclosure programs and activities in general – including caseloads and cycle time. Some of this information may be classified Official Use Only (OUO).

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

Disclosure employees receive paper requests or faxes from other individuals/sources requesting information. A paper folder is created for each request enabling the case worker to work the case and track the progress. However, the information for each request is not imported into the E–DIMS application.

A. The case/project/program file information is received from other IRS functions and/or databases. E–DIMS is not connected to any other database nor does it interface with any other IRS system.

B. Taxpayers do not directly supply any information to E–DIMS unless they are requesting information on themselves. In this case, the taxpayer would provide their full name, Social Security Number (SSN), and the tax period for which they want information.

C. The personally identifying information collected is Identification and Authentication (I&A) username and password. Employee actions taken on cases and time applied are also recorded.

D. Requests for information may be received and logged from any Executive Branch Federal Agency The U.S. Department of Justice accounts for the greatest number of entries on the system in the processing of ex–parte court orders from the US Attorney under IRC § 6103(d) for tax administration purposes.

E. Requests for information may be received and logged from State Departments of Child Support Enforcement, State Departments of Housing, State Departments of Human Services, State Departments of Labor & Industrial Relations State Departments of Social Insurance, State Offices of the Attorney General, State/Local Departments of Employment/Job Services/Human Resources, State/Local Departments of Health and Welfare, State/Local Departments of Public Aid/Assistance, State/Local Departments of Revenue, State/Local Departments of Social Services, State/Local Courts

F. Requests for information may come from taxpayers, tax professionals and members of the public for any information maintained by the IRS. These include requests for specific tax records in the form of FOIA requests, and Privacy Act requests. Records responsive to these requests may be retrieved from any IRS function/office across the Service. Third party records (from outside the IRS) are not accessed or provided.

3. Is each data item required for the business purpose of the system? Explain.

Yes, the data elements are required for the business purpose of the system, E–DIMS uses the data to manage cases, provide inventory control, and provide standardized reporting for the National Disclosure Program.

4. How will each data item be verified for accuracy, timeliness, and completeness?

Data is entered exactly as it is received from the requester. Data validation is accomplished by coding within the system. Personally identifying information about requesters or taxpayers must be maintained when requests involve a disclosure of tax records. However, information provided by individuals is not validated (i.e. missing address or TIN) but transcribed as provided by the taxpayer.

5. Is there another source for the data? Explain how that source is or is not used.
No. This system is only used after a request for disclosure of IRS records is received.

6. Generally, how will data be retrieved by the user?
Data is indexed by case number, which is the primary key within all of the data tables. This is the only unique identifier for each record. This is not a personal identifier but a sequential number for each case entered by an office and the fiscal year of data entry. (i.e., 10–2000–00001). However, secondary data queries may use personal identifiers (Requester Name, Taxpayer Name or TIN) to locate the applicable case number for case retrieval. Paper case files are locally filed by Case Number or Requester/Taxpayer last name so that they may be retrieved by personal identifier depending on the type of correspondence being filed.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, the system will permit searches by requestor's and/or taxpayer's name and Taxpayer Identification Number (TIN) [SSN or Employer Identification Number (EIN)].

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

Role: E–DIMS Users
Permission: Access is given only to those individuals who need to input cases or work on cases. All users are IRS employees, no contractor staff. Attorneys and paralegal staff assigned to Chief Counsel and employees in the Appeals Division have access to E–DIMS for authorized research purposes only.

Role: Manager/Supervisor
Permission: A manager or supervisor is required to authorize new user accounts and assigns data privileges.

Role: Database Administrator
Permission: A database administrator or "superuser" has access to all data within E–DIMS.

Role: Others
Permission: The Inspector General for Tax Administration (TIGTA), System Administrators, and Developers also have limited access to the data in E–DIMS. General Accounting Office (GAO) representatives will have access to E–DIMS during system audits.

9. How is access to the data by a user determined and by whom?
Access to the data within the application is restricted. Users are restricted to only those pieces of the application to which they need access by database roles and to levels of data by profile (i.e. local office, regional data, national data). Users only have access to input data for their office of assignment, run pre–programmed reports and ad hoc queries, and cannot delete data or records, nor otherwise manipulate or physically access the data. Only system developers/programmers actually can manipulate the data tables.

Procedures and controls are documented in the E–DIMS User Guide, the E–DIMS Computer Security Plan, and system development documentation. User profile and roles are assigned by his/her manager on Form 5081, which is reviewed by the System Administrator, and established when user accounts are created.

A user's position and need–to–know determines the level of access to the data. The System Manager and Database Administrator grant approval for system access. A user's access to the data terminates when the user no longer requires access to E–DIMS. Criteria, procedures, controls, and responsibilities regarding access are in the process of being documented in the E–DIMS Security Features User's Guide (SFUG).

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
No – E–DIMS operates from a single server and does not share data with any other IRS system. Data transmissions are encrypted and are not available for use on any other IRS system or within the network.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not applicable.

12. Will other agencies provide, receive, or share data in any form with this system?
No – E–DIMS does not receive information from other agencies for E–DIMS. E–DIMS does receive requests for information from other agencies. Disclosure will input the requester name and taxpayer information in E–DIMS to create a "case" Disclosure that would work. There is no physical connection between E–DIMS and any other application.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
E–DIMS data is approved for destruction 10 years after processing year in accordance with IRM/Records Control Schedule 8 for Administrative and Organizational Records, Item 42 (Job No. N1–58–05–2). Electronic records will be retained for 6 years in a Working Database for active business use, then data will be stripped of all personal identifiers and maintained for an additional four years in an Archives Database to allow for trend analysis and data mining of a statistical nature. Data mining is not currently available but is contemplated for the future. E–DIMS data would be maintained solely for statistical studies as to the volume of requests received in geographical areas, the type and nature of requests received, the length of time to process the correspondence, the grade of the cases worked and the amount of time applied to the cases. Studies of this nature may assist management in the proper allocation of resources to Disclosure programs; and in determining Service compliance with statutory requirements. These efforts can improve program quality and enhance customer service.

14. Will this system use technology in a new way?
No new technologies are used. E–DIMS uses Commercial Off–The–Shelf (COTS) technology for high volume processing of information.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No – E–DIMS does not have the capability to identify, locate, and monitor individuals.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No – E–DIMS does not have the capability to identify, locate, and monitor groups of people based on the information supplied by the requester. However, monitoring of the caseloads and types of requests received by geographic area will allow Disclosure to apply resources where needed and balance caseloads among offices.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No – E–DIMS does not have the capability to identify, locate, and monitor groups of people based on the information supplied by the requester.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No – since E–DIMS captures information maintained by other parts of the IRS in order to respond to requests, there is no new data created. The requestor will utilize the existing appeal rights that are part of the FOIA and Privacy Acts with regard to the information provided to them.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Not applicable. No web visitors are authorized access to E–DIMS. No cookies are maintained on Internet Explorer to track employee access to E–DIMS. Audit trails used for this purpose are maintained on the application server, not on the user PC's.

View other PIAs on IRS.gov