DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUN - 3 2004

MEMORANDUM FOR THOMAS R. HULL
DEPUTY DIRECTOR, COMPLIANCE FIELD
OPERATIONS

FROM: Maya A. Bernstein Linda [illegible]
Privacy Advocate for

SUBJECT: Examination Returns Control System
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the Examinations Returns Control System (ERCS). Based on the information you provided, our office does not have any privacy concerns that would preclude ERCS from operating. A revised PIA is required when considering any major modifications to the ERCS, or at the scheduled recertification of this system/application.

We will forward a copy of the PIA to the Director, Modernization and System Security, to be included in the Certification and Accreditation package for formal acceptance. That office may request information concerning the statements contained in the PIA to ascertain compliance with applicable security requirements.

Note that the Electronic Government Act of 2002 requires that the IRS make this PIA available to the public. If there is any portion of this PIA that you believe would cause harm to the IRS or any party if disclosed to the public, please mark those portions and return it to our office within 10 days.

If you have any questions or would like to discuss this PIA, please contact me at 202-927-5170. Our staff analyst is Priscilla Hopkins at 202-927-9758.

Attachment

cc: Director of Regulatory Compliance

MEMORANDUM FOR MAYA A. BERNSTEIN
PRIVACY ADVOCATE

FROM: Carole Conners, Information Technology Specialist
ERCS Section

SUBJECT: Request for Privacy Impact Assessment (PIA)
Examination Returns Control System (ERCS)

Purpose of the System:

Examination Returns Control System (ERCS) is an inventory system for controlling tax returns and technical time charges for returns under examination at the group level. ERCS provides group managers with a complete system of inventory management reports of all open cases in the group. ERCS allows managers to track statute information, manage inventory by group or examiner, monitor time applied, conduct workload reviews, and determine what type of cases need to be requested.

Name of Request Contact:

Name: Carole Conners
Organization Name & Symbols: ERCS Section, OS:CIO:I:B:CS:ES:ER
Mailing Address: 6635 Executive Circle, Suite 180 Charlotte, NC 28212
Phone Number (with area code): 704.566.5379
Fax: 704.566.5397

Name of Business System Owner:

Name: Bill Hildebrandt
Organization Name & Symbols: SBSE, S:C:CP
Mailing Address: New Carrollton Federal Building 5000
C8-366
Lanham, MD 20706
Phone Number (with area code): 202.283.2268, Fax: 202.283.2257

Requested Operational Date: June, 2004

Category: *(Reason PIA is required--enter "y" or "n" and applicable dates)*
New System?: ___N______
Recertification? (if no change, enter date of last certification) ___Y________
Modification of existing system?: __Y_____

Is this a National Standard Application (NSA)?: _N______
Is this a Modernization Project or System? ___N_____
If yes, the current milestone?: _____ *(Enter 1-5; explain if combining milestones)*

PRIVACY IMPACT ASSESSMENT

NAME OF SYSTEM AND ACRONYM: Examination Returns Control System (ERCS)

DATA IN THE SYSTEM:

1. Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.

The Examination Returns Control System (ERCS) is an inventory system for controlling tax returns and technical time charges for returns under examination. In order to link returns under examination to the Audit Inventory Management System (AIMS), the following types of taxpayer data are stored in ERCS: Taxpayer Identification Numbers (TIN), Employer Identification Number (EIN), Taxpayer/Employer Name, Taxpayer/Employer Address, and related return information, such as amounts claimed by taxpayer filing an amended return or claim (which is required by SBSE and LMSB), Secondary SSN, and Activity Code, Source Code, Status Code, and Name Control. Additional information is contained in the database, which is locally defined, to allow users to classify, type, and track returns and local projects. Assessment amounts are also stored for closed returns. This data does not appear on reports available to end-users or managers, but only to functional coordinators. Reports dealing with closed returns do not include information about the examiner. The definitions or meanings for these locally defined data items are stored in local files on the system.

ERCS also contains information on employees in the Exam division. For the purpose of recording time charges, information such as the AIMS Assignee Code (AAC), Position Code, and Unique Employee Identification Number are stored in ERCS. The Unique Employee Identification Number is a sequence number generated by the ERCS application. This number is in a format required by the Summary Examination Time Tracking System (SETTS), which is a downstream mainframe program. The ERCS application does not use an employee's SEID number but stores the employee's SSN. This is required for security purposes and is used to see if an employee attempts to access his/her own return or spouse's return. At the end of each time cycle, this information along with a summary of the employee's time charges for the cycle is electronically transmitted to the Summary Examination Time Transmission System (SETTS). Employee Name and Social Security Number (SSN) are stored for inventory control purposes (including controls to prevent unauthorized access to employee returns under audit). Additional information, such as the employee's Aims Assignee Code, POD, position code, position code date, prior position code, grade, prior grade, employee's date of activation on the ERCS system, and duty hours, are stored on each employee accessing the ERCS programs and is used to control user access to the ERCS menu system and to control access to the data itself. Also, this data is maintained for time purposes. The prior grade and prior position code are retained because an employee's grade or position code may change in the middle of a SETTS cycle.

2. What are the sources of the information in the system?

Examination records (taxpayer) are added and updated in the system in two ways: one through weekly processing of a file, extracted from the Audit Inventory Management System (AIMS) database, against the ERCS database, and second, users may add and update records through programs contained in ERCS. All information for manual input comes from taxpayer records and IRS employees.

Data is uploaded to ERCS from the Midwest Automated Compliance System (MACS). The data from MACS include: TIN, MFT, tax period, activity code, name control, taxpayer name, primary business code, secondary business code, employee group code, source code status code, tracking code, project code, return label flag (ON/OFF), special message code, aging reason and TIN type. Only Planning and Special Programs (PSP) users can execute this menu option to upload MACS data to ERCS.

Time charges are entered on the system by the secretary or clerk in each applicable function (i. e. Group, PSP, Quality Management Staff (QMS)) from the agent's input document (i. e. Exam Technical Time Report, Form 4502 or ERCS Tax Auditor Daily, Form 4606).

3. How will data collected from sources other than IRS records and taxpayer, if applicable, be verified for accuracy?

N/A

4. Are the data elements described in detail and documented?

The data elements used in ERCS are described in detail in the ERCS Technical Reference Manual. See the attachment of the ERCS Database chapter for a copy of the data elements.

ACCESS TO THE DATA

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

Users and Managers have restricted access to the data through the ERCS programs. Access for these users is based upon the individual requirements of each user. The ERCS Functional Coordinator who is the liaison between the Examination Division Users and the Information Systems Staff in each area sets up users. ERCS Audit Trails are created for updates to the database based on recommendations by the Treasury Inspector General of Tax Administration (TIGTA).

System Administrators are generally not given access to the data through the ERCS programs. The Functional Coordinator has the ability to grant temporary access or deny access for the System Administrator to the database.

The developers may be granted temporary access to the database for problem solving purposes.

The ERCS Functional Coordinators (usually examination personnel) have access to the data in the ERCS database. However, audit trails are created for data changes through the programs and changes to fields on an IRS employee's return that identifies the return as an employee audit return. This causes messages to be written to the Security Officer.

2. How is access to the data by a user determined?

User access is setup by the ERCS Functional Coordinator based upon the User's duties and responsibilities. For example, a group secretary would have permission to add and update records and run reports on ERCS in his/her group as long as the records were in a group status. The same group secretary would have limited research capabilities to locate where a return is in the area.

A user must complete an online 5081 to be allowed a XXXX login to ERCS. Once the 5081 is approved, the Systems Administer at Tennessee Computing Center (TCC) creates the XXXX login/password and adds the user to the ERCS menu database, which allows access to a specific SBSE area database, or the LMSB database. The manager contacts the Functional Coordinator as to what the group code is for that user. The FC adds the user to ERCS allowing only the users assigned group codes. This step does not involve the use of a 5081, and is administered by SBSE and LMSB managers and coordinators. Below is a list of valid TIN formats and any other format is invalid including negative TINs:

##-#######N	Non-master File Employer Identification Number
##-#######	Business Master File
###-##-####N	Non-master File Social Security Number
##-##-####	Individual Master File
###-##-####*	Invalid Social Security Number on Individual Master File
###-##-####V	Valid Social Security Number on Business Master File
###-##-####W	Invalid Social Security Number on Business Master File
#########-D	Temporary Taxpayer Identification Number

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

The user's access is restricted. Users may only update records on ERCS within their control. They also have limited research capabilities on the ERCS system. Users researching records outside the user's control may result in "research audit trails" being created.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

Users are individually restricted by the ERCS programs from adding or updating returns outside the realm of their permissions. Employee Audit Security Features are included in the system to restrict access to employee audit returns except to those individuals directly responsible for the audit. ERCS Audit Trails are created for updates to the database based on recommendations by TIGTA. This includes additions and updates to records as well as research audit trails.

The Employee Audit Security Feature has special restrictions in place to protect the privacy of IRS employees when their returns are under audit. When a return is added, changed, reactivated to ERCS, either by a user or by batch processing, the TIN and the secondary SSN on the return are checked against the ERCS employee database table for a match on an active employee's SSN. If a match is found, the EMPL_AUDIT flag is turned ON in the record. When this flag is on, the user does not have access to their return. The audit information is written to dated binary files. The Read Audit Trails program provides ERCS FCs with a way to read the audit files and generate reports based on various selection criteria. Limited information is displayed. Only TIGTA downloads all audit trail data to an Access database to analyze the data. This data is compressed into a "zip" file, which is a binary file. The file is sent to a specific computer and must login with a password. If this computer is unavailable or the password is invalid, the program aborts. This entire process is automated.

The ERCS programs will terminate the user's login session and write a notice to the Security Officer if a user in the wrong XXXX group attempts to access the ERCS main menu system. There is an exception for the ERCS Functional Coordinator. The ERCS programs will not terminate the login session for this user, but they will prevent program access until the user changes to the proper XXX group. (Permissions to change UNIX groups must be granted by the System Administrator.)

All users accessing the ERCS programs must have an ERCS employee record with a valid login name. The programs capture the login name of the user and search the ERCS employee file for a match. If a match is not found the user is denied access to the programs. This applies to all users including Charlotte Development Center (CDC) Developers.

Users must be given permission to access the database. This is a requirement of the database management system (DBMS) on the XXXX XXXXX system. The ERCS main menu prevents users from accessing ERCS if they do not have permission for the database. The ERCS Functional Coordinator is responsible for making sure the users have been granted access to the ERCS database.

The system database audit trails must be on prior to the users accessing the ERCS main menu. The programs will not execute if the audit trails are off.

There is a special lock out feature of ERCS that allows the ERCS Functional Coordinator or the System Administrator to prevent accidental access to the ERCS system by users if a need arises or when batch processes are scheduled to run. ERCS FCs are SBSE employees located nationwide who hold the key to the success of ERCS programs. The coordinator's job includes assisting end-users, monitoring how the system is used, determining each user's permissions, setting up new users, maintaining local files and serving as a starting point for many questions. The ERCS FC serves as a liaison between end-users and MITS.

Systems Administrators are computing center MITS employees, and are responsible for the smooth operation of the ERCS computer. SAs are responsible for administering user logins and passwords, maintaining and tuning the computer and database management system, installing new versions of ERCS and making sure system and database backups are done.

The ERCS menu system is setup so each type of user receives the menu selections that correspond to the duties the user is expected to perform. There are 8 types of ERCS users. Within each user type, data access is defined further by the ERCS Functional Coordinator and by the type of permissions each user is given. Permissions may be restricted by status code, AAC, and may only be granted for read or for read and write. Users with a manager's position code may be granted permanent permission to approve additions and changes to the database within their control. Technicians and the ERCS Functional Coordinator may be granted temporary approval permissions to serve as a backup when the manager is unavailable. Temporary permissions may also be granted to a user by the manager or the ERCS Functional

Coordinator. Audit trails are written for all permission changes through ERCS. The audit trail contains the login of the person who made the changes as well as information about the change.

Employee audit security features in ERCS prevent any user from accessing an employee audit return unless the user has permission to update the return. ERCS prevents employee audit returns from being added to the ERCS database if the return should not be audited in the area (i. e. Planning and Special Programs (PSP) manager, Exam manager, etc.). ERCS also prevents employee audit returns from being assigned to the same group the employee under audit is assigned. Research on employee audit returns is not permitted in ERCS. Any unauthorized access to an employee audit return will result in a message sent to the Security Officer.

5. Do other systems share data or have access to data in this system?

Data comes into ERCS by manual inputs of the users and by regular downloads of information from the Audit Inventory Management System (AIMS) database and the Midwest Automated Compliance System (MACS). Each week, information is extracted for each area into an AIMS database and compared to the ERCS database. A complete comparison is done for each return in the file. When differences are found, a determination is made as to which system is more current, and the appropriate updates are submitted to bring the databases into agreement. Each day, requisitions and updates manually input into ERCS are automatically uploaded to AIMS through the Information Data Retrieval System (IDRS). Since the ERCS Uploading program uses the Generalized Interface made available by the National Office, all IDRS security features remain in effect. This two-step process insures consistency between the ERCS and AIMS databases.

Weekly, data is downloaded from MACS to ERCS. The ERCS data is then compared to the AIMS data and if there is a difference, a determination is made as to which system is more current. Then the appropriate updates are submitted. Also, data is downloaded from ERCS to MACS. The MACS computers are C-2 certified so all MACS security features remain in effect.

6. Will other agencies share data or have access to data in this system?

No.

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes, the use of the data is both relevant and necessary to the purpose for which ERCS has been designed. ERCS has been in existence for approximately 20 years. It has automated activities that were previously done manually. Examination return information is stored on the system to allow ERCS to be used for an inventory system for returns under examination in the area. The information is used to create IDRS command codes to be uploaded to AIMS; for inventory, statute, time and monitoring reports; to schedule appointments and for comparison to the AIMS data. During weekly processing of an AIMS data file against the ERCS database, reports are generated to alert the ERCS users of discrepancies to be corrected either on ERCS or AIMS. The record with the most current data determines whether ERCS or AIMS is updated.

The program assumes if a record is under ERCS control, the user makes changes to the record on ERCS and not AIMS. The opposite is assumed if the return is not under ERCS control.

Technical time charges are stored on the ERCS system and uploaded to SETTS each cycle. The information is also used for creating various types of time reports used by the group manager to determine overage cases, high time cases, etc.

Employee information is stored on the ERCS system to link employees with their inventory, to produce the SETTS file, and to prevent unauthorized access to the system and employee returns under audit.

Local files and national files are stored to identify, define and validate codes used in the database.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No, the system does not derive new data or create previously unavailable data about an individual.

3. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use? If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

The data is being consolidated from XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. As a user logs into the database, the front-end menu sets the area allowing the user to only see the area for which he/she has permission. The IS support staff is responsible for maintaining the users and areas for which they will have access. Also, the IS support staff is responsible for controlling user access to the ERCS XXXXXXXX system. This normally means adding or deleting users from the system and developing and maintaining a front-end menu that users log into. The IS staff is responsible for maintaining the XXXX group permissions on the ERCS executable, files, and directories. The ERCS Functional Coordinator is responsible for setting the user access within the database based upon user function (group user, territory managers, PSP user, ESP user, QMS user) once the IS staff has established a user on an ERCS XXXXXXXX system. No ERCS user is added to the XXXXXXXX without receipt of Form 5081, Automated Information System (AIS) User Registration/Change Request. It should be noted that the ERCS XXXXXXXX computers use the XXXX XXXXXXXXXXXX and the Commercial Security Package, thus satisfying the requirements of C2 security. Only the ERCS Development Center in Charlotte, NC has access to the program code. Therefore, no user can change what data is input or received from AIMS. No processes are being consolidated.

4. How will the data be retrieved? Can it be retrieved by personal identifier? What are the potential effects on the due process rights of taxpayers and employees?

To access the data, a user must first log into their area's ERCS system, generally using a PC acting as a dumb terminal. Once the user has logged into ERCS, the user can request, update, close and reassign records that the user has permission to access. These activities would require retrieval using personal identifiers, i.e. taxpayer name or TIN. Users can generate reports contained within the program for AIMS assignee codes which they have permission. These reports allow for the monitoring of returns in a group's or an employee's inventory. Access to the data contained in ERCS has no effect on the due process rights of taxpayers and employees.

MAINTENANCE AND ADMINISTRATIVE CONTROL

1. Explain how the system and its use will ensure equitable treatment of taxpayers and employees. Explain any possibility of disparate treatment of individuals or groups. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The ERCS system is operational in one site, on XXX XXXXXXXX system and accessed by each area. This system consists of XXXXXX, which includes all areas and A/C International. The program provides consistency. Only the ERCS Development Center in Charlotte, NC has access to the program code. Therefore, no user can change the program to change what data is input or received from AIMS. The system is used for inventory control in Examination Division. It neither ensures equitable treatment nor provides opportunities for disparate treatment of taxpayers, groups, individuals or employees.

2. What are the retention periods of data in this system? What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

Archiving of old records is done approximately every quarter. During weekly AIMS tape processing, records on the "exmf" table in the ERCS database, which are no longer on the tape, are flagged for archiving if they meet any of the following criteria:
-- it is in a 5000-series employee group code (EGC) which is Campus Correspondence Examination Groups
-- it is in status 90 (closed return) and has been closed from the group for more than 400 days
-- it has an EGC contained in the local file "class_cf_aac", the employee id is zero and no time has been charged to the return

In addition, records that have a TIN that is negative or has more than 9 digits are archived.

Records on the "tapp" database file, the time files, are archived if they meet the following criteria:
-- if a DET record (direct exam time) has no corresponding "exmf" record and the time charge date is more than 400 days past.
-- if a Non-DET record has a time charge date that is more than 400 days past.

Records closed in status 90 are written to the "hist" table. Records in the "hist" table are archived after 1100 days (approximately 3 years).

Archive tapes are stored and purged following local operational host site procedures. Complete documentation is located in the ERCS Technical Reference Manual. Retention periods for ERCS data is listed the ERCS Technical Reference Manual as described in the IRM 2.7.4 and IRM 2.7.6.

3. Is the system using technologies in ways that the IRS has not previously employed?

No.

4. Will this system provide the capability to identify, locate and monitor individuals? Groups of people? What controls will be used to prevent unauthorized monitoring?

ERCS is an automated inventory management system used by Examination Division for controlling tax returns and technical time charges from the time returns arrive in the area until they are closed on AIMS. It does not provide the capability to identify, locate or monitor individuals or groups.

5. Under which Systems of Record notice (SOR) does the system operate?

ERCS operates under the same SOR as the Audit Information Management System, AIMS, SOR 42.008 and Treas/IRS 34.037 covers the audit trail.