



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

DEC 24 2003

MEMORANDUM FOR MARK MAZUR
DIRECTOR, RESEARCH ANALYSIS AND STATISTICS

FROM: Maya A. Bernstein
Privacy Advocate 

SUBJECT: Internal Revenue Manual Electronic Clearance
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the Internal Revenue Manual Electronic Clearance (IRM E-Clearance). Based on the information you provided, our office does not have any privacy concerns that would preclude IRM E-Clearance from operating. However, a revised PIA is required when considering any future upgrades or major modifications, 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 for operation. That office may request information concerning the statements contained in the PIA to ascertain compliance with applicable security requirements. If you have any questions, please contact me at 202-927-5170; or Priscilla Hopkins at 202-927-9758.

Attachment

cc: Director, Modernization and System Security OS:MA:M

MEMORANDUM FOR MAYA A. BERNSTEIN
PRIVACY ADVOCATE

FROM: /s/ Susan B. Novotny
Director, Servicewide Policy, Directives and Electronic
Research RAS:SPDER

SUBJECT: Request for Privacy Impact Assessment (PIA) –
*Internal Revenue Manual Electronic Clearance (IRM
E-Clearance)*

Purpose of the System: The Internal Revenue Manual (IRM) clearance process will be streamlined by applying automated workflow and electronic document management functionality to the current business process. Workflow and electronic document management capabilities will reduce the cycle time required for reviewing and approving revisions to the IRM.

The IRM author/originator will complete an electronic Document Clearance Record (DCR) to identify required document reviewers. Emails will automatically be generated to alert reviewers of necessary tasks and alert authors of progress on reviews. Authors will review a summary of reviewer comments and incorporate necessary changes back into the revised IRM file.

Workflow tracking and an electronic document management system will provide increased document clearance uniformity and accountability, and improved document oversight and routing. The DCR will provide the status of reviews and identify what reviewing offices have completed or not completed the IRM review.

Name of Request Contact:

Name: Susan Charlton

Organization Name & Symbols: Servicewide Policy, Directives and Electronic Research, RAS:SPDER

Mailing Address: 1111 Constitution Ave. N.W., Washington, D.C. 20224

Phone Number: (202) 927-5675

Name of Business System Owner:

Name: Susan B. Novotny

Organization Name & Symbols: Servicewide Policy, Directives and Electronic Research, RAS:SPDER

Mailing Address: 1111 Constitution Ave. N.W., Washington, D.C. 20224

Phone Number: (202) 927-5761

Requested Operational Date: Conduct pilot - May 2004

Category: (Reason PIA is required--enter "y" or "n" and applicable dates)

New System?: X

Recertification? (If no change, enter date of last certification) _____

Modification of existing system?: _____

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)

System of Records Number(s) (SORN) #: A SORN is not required as the standard practice for retrieving information is by the IRM number, not by employee name. The audit access log is covered by the SOR entitled Treasury/IRS 34.037, the IRS Audit Trail and Security records system.

Attachment: PIA

cc: David Silverman

Data in the System

<p>1. Describe the information (data elements and fields) available in the system in the following categories:</p>	<p>Taxpayer: None</p> <p>Employee: NT User Login Phone Number Office Symbol Email Address Originator's Manager Name Originator's Manager Email Address Originator's Manager Phone Number NT User Login Action Action Date</p> <p>Other: Approval Date Delegation Date Comment Comment Date Submission Date Resubmission Date Request Date Completion Date Decline Date No Impact Date Document Number Document Title Reviewing Organization Title Reviewing Organization Symbol</p>
<p>A. Taxpayer B. Employee C. Audit Trail Information (including employee log-in info) D. Other (Describe)</p>	

<p>2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.</p> <ul style="list-style-type: none"> A. IRS B. Taxpayer C. Employee D. Other Federal Agencies (List agency) E. State and Local Agencies (List agency) F. Other third party sources (Describe) 	<p>The employee NT User Login is supplied by the employee when entering the application. The application will verify the existence of the login in the existing IRS Corporate Authoritative Directory Service (CADS) database. The application will obtain the employee phone number, office symbol, email address and name of manager from CADS to auto-fill data fields on the electronic Document Clearance Record (DCR). The employee has the ability to edit the DCR if information is not correct.</p>
<p>3. Is each data item required for the business purpose of the system? Explain.</p>	<p>A paper Document Clearance Record (DCR) currently is used to obtain reviewer comments and approvals of revisions to the Internal Revenue Manual (IRM). The DCRs are maintained to provide a historical record of the clearance and approval of all IRMs. The electronic system collects the same information.</p>
<p>4. How will each data item be verified for accuracy, timeliness, and completeness?</p>	<p>The employee verifies personal information provided by the CADS database and has the ability to update the data on the DCR.</p>
<p>5. Is there another source for the data? Explain how that source is or is not used.</p>	<p>No</p>
<p>6. Generally, how will data be retrieved by the user?</p>	<p>Data will be stored and retrieved by the IRM number.</p>
<p>7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?</p>	<p>No</p>

Access to the Data

<p>8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?</p>	<p>All users and system administrators of the application have read only access.</p>
<p>9. How is access to the data by a user determined and by whom?</p>	<p>Data is stored and accessed by IRM number. Any user identified as a reviewer by the author of the IRM has read access to the data. Archived data is available to all IRS employees for historical research.</p>
<p>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. If NO, continue to Question 12.</p>	<p>Yes. Employee data (employee NT login, phone number, office symbol, email address, manager name) is obtained from CADS.</p>
<p>11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?</p>	<p>Yes</p>
<p>12. Will other agencies provide, receive, or share data in any form with this system?</p>	<p>No</p>

Administrative Controls of Data

<p>13. What are the procedures for eliminating the data at the end of the retention period?</p>	<p>All data will be archived to fulfill historical IRM research requests. IRM Exhibit 1.15.36-1 (Cont. 22) provides for the permanent retention of "Directive Case Files" for the Internal Revenue Manual. The IRM Librarian will establish on-site retention periods for the electronic records. The electronic records will periodically be reduced to microfilm for permanent retention by NARA as required by IRM Exhibit 1.15.36-1.</p>
<p>14. Will this system use technology in a new way? If "YES" describe. If "NO" go to Question 15.</p>	<p>No. The application will reside on the IRM intranet.</p>
<p>15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.</p>	<p>No</p>
<p>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.</p>	<p>No. The application allows the originator of the document clearance record to monitor the review process by organization(s) assigned to review the document. This allows the originator to track the document review status.</p>
<p>17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.</p>	<p>No. The application will provide uniformity to the IRM clearance process.</p>

<p>18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?</p>	<p>No impact on due process exists in this system. A document reviewer may provide the originator of the document comments during the review process and decline to approve the document until review comments are addressed. The originator must address reviewer comments before proceeding with the document clearance.</p>
<p>19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?</p>	<p>No persistent cookies are used. One session cookie stores information that the current user was authenticated during the login process. No user id is recorded in the cookie.</p>