




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

MAY 06 2004

MEMORANDUM FOR MARK J. MAZUR
DIRECTOR, OFFICE OF RESEARCH, ANALYSIS AND
STATISTICS

FROM: Maya A. Bernstein 
Privacy Advocate

SUBJECT: National Research Program
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the National Research Program (NRP). During the course of our review, we identified a potential privacy and security risk due to multiple roles assigned to the system administrator. However, based on the information you provided and discussion with your staff, we are satisfied that this risk is small, and therefore our office does not have any continuing privacy concerns that would preclude NRP from operating. A revised PIA is required when considering any major modifications to the NRP, 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 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

PRIVACY IMPACT ASSESSMENT

NATIONAL RESEARCH PROGRAM

April 1, 2004

Rev. 1

I. Data in the System

The goal of NRP is to design and implement a successful strategy to collect data that will be used to measure payment, filing and reporting compliance and to deliver the data to the Business Operation Divisions to meet a wide range of needs. The guiding principles for NRP are:

- Minimize taxpayer burden as data are collected.
- Ensure that the collected data will meet business objectives and are used as a corporate asset.

The IRS will also use the NRP to analyze taxpayer compliance and to assess the effectiveness of compliance programs and treatments in use by the IRS.

What IRS files and databases are used?

The NRP system received input from the SCRS, which were transmitted weekly from MCC to DCC beginning with cycle 4 in January 2002 through the last cycle of the tax year. The EOAD data is received on a periodic basis beginning in the fall of 2002. Procedures to transmit this data to DCC have been established and documented.

The reported items to be verified were obtained from sources at the Martinsburg Computing Center and loaded into the NRP database at DCC. The two major sources of return data are the SCRS and the TRDB data. For some sample returns, it was necessary to transcribe additional data to supplement the data provided by SCRS. To secure data fields not originally captured in the 1040 return pipeline, data transcription of additional fields on Schedules C, D, E, F, 2106, SE and EIC, as well as, additional fields on the 1040 to include dependent SSN information, were necessary. The ADC will secure data fields from the following forms and schedules: Schedules K-1 – 1041, K-1 – 1065, K-1 - 1120S, Forms 4797, 4952, 6251, 6252, 4562, 8582, 8829, 4835, 6198, 4684, 1116, 8863, 8606, 8801, 6781, 8824, 8586, and 5329.

Other internal data to include the additional transcribed schedules, RTF, IDRS, CBRS, MACS, DDB, Choice Point were associated with the sample returns to facilitate the verification of return accuracy. In addition, demographic data was used against TCMP data, specifically zip code, as a method to determine the workload distribution of the sample selected returns by examination site for estimation of required resources. The IRS has refrained from using demographic data, such as age, gender, religion, race, ethnicity or national origin in research efforts that may suggest specific groups for enforcement activities. For audited sample returns, audit results are collected

from the Report Generation System (RGS) and the Exam Operational Automation Database (EOAD). NRP tracks the status of all sample returns from their initial selection to the recording of verification results.

A transcription application using Access and a SQL server resides in Austin. The required supplemental fields update the DCC NRP database. Transcription data formats are validated at Austin with consistency checks of transcribed fields against posted return data also being performed. Additionally, resultant EOAD data, i.e., adjustments, is consistency-checked against corrected fields on the database at DCC prior to loading. The ADC transcription application will use Access and a SQL server residing in the Cincinnati Service Center. The transcribed supplemental fields will update the DCC NRP database. The transcription application will verify the accuracy of the input data through original entry (OE) and key verification (KV). The additional transcribed fields will not run through any consistency checking process and therefore will not be used to make any adjustments to other captured sample data.

The process of associating other internal data with sample returns is as follows. Case folders of tax return and other data were assembled at the Case Building Site located in Austin Texas, the AUCC. When all pertinent data was assembled, the case was reviewed by experienced examiners and forwarded, if necessary, for verification of reported items.

All data (items reported by the taxpayer, other data, e.g., 1099s and prior year return data, and adjustments based on return verification) were collected for each sample return and loaded into the NRP database at DCC. All data, except for the "other" data, was tested to ensure that data input and other errors were identified and corrected. Data consistency programs are used to verify the integrity of the data for both input accuracy and consistency among related fields on associated return data.

IS/Core Services Branch has developed Case Tracking Software which allows access to the NRP database for authorized users via the Intranet. The CTS record contains the SSN and the case number. The SA uses the SSN to associate case building and return data to the one common case number. The SA, classifiers and auditors update the CTS record to show the status of the case through the case building, classification and examination process. Once the examination is complete and the audit result data is sent to DCC, the SA at DCC completes the CTS record indicating the last piece of data has been received and associated to the case. At this point there is no access to this CTS record with the exception of the SA for administrative purposes or error correction purposes. Research type users will never have access to the CTS record. There is no requirement for this situation. The point that the resultant audit data is placed in the database, the Research portion of the study can start and the research user's view is of sanitized data and available based on the NRP Director's approval. The case tracking application is in place and included in the Security Certification process. It lets the user track the status (receipt, transfer, exclusion, etc.) of cases. It also provides for online error correction and reports for authorized users.

1. Generally describe the information used in the system in each of the following categories:

-
- Taxpayer: The sample includes about 50,000 individual income tax returns filed in 2002 with a tax period ending 200109 through 200208. This is not the 1040 tax period, but the study tax period. The sample does not include international, APO/FPO, amended/corrected, and certain other returns. The principal data collected about these returns includes the information listed in Appendix 8:

- Form 1040, 1040A, 1040EZ
- Schedule-A Itemized Deductions
- Schedule-C Profit or Loss from Business
- Schedule-D Capital Gains and Losses
- Schedule-E Supplemental Income and Loss
- Schedule-F Profit or Loss from Farming
- Form 2106-Employee Business Expense
- Schedule SE – Self-Employment Tax
- Schedule EIC – Earned Income Credit, Qualifying Child Information
- Information Returns Master File (IRMF)
- Audit results (RGS, EOAD, and examiner workpapers)

The principal data to be collected about these returns through the ADC will include the following:

-
- Schedule K-1 – 1041
- Schedule K-1 – 1065
- Schedule K-1 - 1120S
- Form 4797 - Sale of Business Property
- Form 4952 Investment Interest Deduction
- Form 6251 - Alternative Minimum Tax
- Form 6252 - Installment Sale
- Form 4562 – Depreciation
- Form 8582 - Passive Activity Loss
- Form 8829 - Business Use of Home
- Form 4835 - Farm Rental Income
- Form 6198 - At Risk Limitation
- Form 4684 – Casualty and Theft
- Form 1116 - Foreign Tax Credit
- Form 8863 - Education Credit
- Form 8606 - IRA/Cloverdale
- Form 8801 - Prior Year Minimum Tax
- Form 6781 - Gains/Loss from Contracts
- Form 8824 - Like Kind Exchanges
- Form 8586 - Low Income Housing
- Form 5329 - Retirement Plans Tax

- **Employee:** Employee data used in the DCC system consists of User Identification (ID), Location Code, Badge Number, Last Name, First Name, Phone Number, Position Code and Email Address. The data is taken from the Form 5081 the employee must submit to access the system. The phone number and email address is used to communicate with system users. IS Security guidelines require that the above listed user information be stored in the system for identification purposes for every user of the system. This data is manually input by the System Administrator (SA) one time. At the same time the SA identifies the level of access and views authorized for this user. After the SA records the information in the system, the user is only required to enter a login and password to access authorized information.

For users of the RGS System at the AUCC, all of the listed data except the employee email address is currently stored in the RGS system by the users. The employee physically enters this information in the "User Setup" and "User Contact Information" tabs area of the RGS system when the user first sets up their computer. This information is then automatically associated with each subsequent case file. When updates are necessary such as change of phone number, etc. the user must physically update this area on their RGS computer system again. The user enters this information manually the first time only. Subsequent access requires just a login and password. This login validation is required for all users of RGS.

- **Other:** Choice Point data was used to validate certain information on the tax return. This data was further validated during an audit (either correspondence or face-to-face) to solidify accuracy. (See Attachment 5 for ChoicePoint Data fields) Net Basis data was used to calculate and validate the stock equity of data reported on the tax return's Schedule D. Net Basis is not queried by any personal identifier. The Net Basis data used strictly the case tracking number in order to request the data from Net Worth Services and to associate the data back to the case file when it was received back from Net Worth Services. There is no other taxpayer information contained in these data transmissions.
- **Web Server:** No taxpayer data or other data described above will be displayed on the NRP website or collected in the NRP web server databases. Employee data will be displayed on the website in the form of employee directories of NRP staff, RGS and NRP Coordinators, Territory Managers, and Headquarters Subject Matter Experts for contact information purposes only. Employee diagnostic surveys will be conducted via the web server and the results captured and stored in the web server databases. No specific employee data is captured, only survey results. The survey result databases are not accessible through the NRP website and are only accessible by the NRP database administrator for summary purposes. The website is an internal intranet site not accessible by the general public. Access to the NRP website requires a valid LAN login and password to access the IRS intranet. The NRP website does not require revalidation of the LAN login and password and relies on NT or XP account validation. The NRP website contains sensitive, official use only information. NRP IRMs are posted on the website for access by NRP examiners, managers, coordinators and classifiers. All

information posted to the NRP website goes through a review and approval process by subject matter experts and NRP management to ensure its accuracy and necessity.

• *What are the sources of the information in the system?*

The system obtains information from internal sources (IRTF, SCRS, TRDB, IRMF, CBRS, etc.) and external sources (Choice Point, Net Basis, and directly from the taxpayer).

a. *What IRS files and databases are used?*

The NRP system receives input from the SCRS, Return Transaction File (RTF), Information Returns Master File (IRMF), TRDB, and EOAD. The RTF, SCRS, and TRDB files were transmitted weekly from MCC to DCC beginning with cycle 4 in January 2002. The EOAD data is received on a periodic basis beginning in the fall of 2002. Procedures to transmit this data to DCC have been established and documented. See Appendix 8.

b. *What Federal Agencies are providing data for use in the system?*

We are using SSA information acquired through the IDRS command codes DDBOL, DDBKD, and DUPOL that is required by law to be provided to the IRS for use in EITC type examinations. Attachment #4 to this document is the MOU with HHS/SSA and the IRS. See Attachment 8 for more database information.

c. *What State and Local Agencies are providing data for use in the system?*

We use state acquired information provided to SSA through the IDRS command codes DDBOL, DDBKD, and DUPOL.

d. *From what other third party sources will data be collected?*

Data was provided from Choice Point Inc. and Net Worth Services, Inc. using the Net Basis 2000 service.

Choice Point is a data gathering application that was useful in the NRP casebuilding process. The value of Choice Point is its ability to validate what's on the return, i.e., the presence of spouse data from Choice Point = filing status code on return. See Appendix 8 for more Choice Point information.

e. *What information will be collected from the taxpayer/employee?*

NRP collects data on sample returns through the RGS/EOAD system. The data includes examiner data as described in question 1. The data also includes taxpayer data consisting of audit results from EOAD or RGS and the examining officers' narrative to accompany

issue(s), and any other taxpayer specific information including copies of taxpayer contracts, bank statements, etc., acquired during the course of the examination and used to provide support to their determinations. The RGS servers in AUCC are populated with RTF data from MCC. Once the case has been closed through AIMS, the RGS data is deleted from the AUCC RGS servers and transmitted to DCC and loaded in the DCC NRP database. Identification of taxpayer data on the DCC server has been addressed in another section of this PIA.

3. a. *How will data collected from sources other than IRS records and the taxpayers be verified for accuracy?*

Verification of data collected from both internal IRS sources and outside the NRP examiner will make sources during the course of the examinations to the extent any of this information is determined to be relevant for purposes of verifying the accuracy of a sample return. The taxpayer will verify this data and the taxpayer will have the opportunity to contest the validity of the data. Data from sources other than IRS records and the taxpayer that are determined to be inaccurate is not corrected by the IRS. This data is marked as invalid or inaccurate with the examination's justification and is not considered a viable data source for this particular case.

b. *How will data be checked for completeness?*

All data used as part of the NRP study will be verified for completeness and timeliness by the taxpayer and to the extent that the IRS has other resources to validate the data. Data that is considered incomplete and cannot be verified by the IRS will not be used to make any determination against the taxpayer. Although ChoicePoint data may be one factor in the determination to audit a taxpayer, it may also result in a determination not to audit. For example, if the tax return has a loss on Schedule C, and ChoicePoint indicates that the taxpayer may have filed for bankruptcy due to business failure, it is evidence that the loss is proper. Therefore, the classifier and examiner may accept the loss as filed. If the bankruptcy information was not available, the classifier or examiner may have identified the Schedule C loss as a possible issue. Nevertheless, all data will be verified with the taxpayer, to the extent possible, before any deficiency is assessed against them.

Is the data current? How do you know?

Attachment #5 is the schedule of updates to the input sources used by Choice Point. The examiner would need to verify any discrepancies noted by the taxpayer that fall outside of the update schedule.

4. *Are the data elements described in detail and documented? If yes, what is the name of the document?*

The data elements for the NRP system and the ADC system are described in detail and documented using Microsoft Excel spreadsheets. The names of these documents are NRP Data Element Map (attachment #1) and NRP ADC Data Element Map (attachment #6).

II. Access to the Data

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

IRS internal users with access to the data are the System Administrators, Database Administrators, Developers (Developers need access to write programs that will be used to provide views to specific data tables for approved users, create reports on the resultant data, and then test the applications with the data to ensure they are working properly) , Functional Security Coordinators, National Office Analysts, Case building personnel, returns processing personnel, Operating Division personnel, and NRP coordinators. Developers at the National Office and returns processing personnel may include contractors with security clearances. All developers at DCC are IRS employees. All personnel who have access to NRP have filled out Form 5081 and are granted access only to those areas that are required for them to perform their duties. Their access is immediately revoked when it is no longer required. Only Administrators and developers full access to production data. The other personnel listed above have read access to production data with limitations set by the database views they need access to.

2. *How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?*

Access to the data within the system is restricted. Internal users are restricted to only those database views to which they need access.

Procedures and controls shall be documented in the NRP Computer Security Plan, 2001, and system development documentation. The administrative user's profile and roles are assigned by his/her manager on IRS Form 5081, which is reviewed by the NRP System Administrator, and established when user accounts and permissions are granted.

A user's position and need-to-know determines the level of access to the data. The System Manager and System Administrator (managers approve access through the 5081 process and the SA carries out the steps to grant approval to the appropriate data per the 5081) grant approval for system access. A user's access to the data terminates when the user no longer requires access to NRP. Criteria, procedures, controls, and responsibilities regarding access are documented in the NRP Security Features User's Guide (SFUG).

The following mandatory rules are defined for users of all IRS computer and information systems:

- Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties.
- Users are restricted to only accessing, researching, or changing accounts, files, records, or applications that are required to perform their official duties.
- Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of famous or public persons unless given authorization.
- If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. Users will be held accountable if they access an unauthorized account.
- Users are required to protect passwords from disclosure and to refuse acceptance of passwords that are not delivered in a sealed envelope. Users are required to log/sign off anytime they leave the computer or terminal.
- Users are required to retrieve all hard copy printouts in a timely manner, ensure that magnetic media is secured based on the sensitivity of the information contained, and that they will practice proper labeling procedures. Users are instructed not to disclose or discuss any IRS-related information with unauthorized individuals.
- Users are instructed to protect IRS employee internal work from disclosure.
- All vendors are to be escorted and monitored.

The NRP system requires all users to identify themselves and provide proof of their identities by user identification (USERIDs) and passwords. USERIDs and passwords are unique to each internal user.

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

Currently, the DCC developers have access to all data on the NRP system. All other access is restricted. All other NRP users have limited access. Access must be positively granted by management based on the employee's need-to-know and job duties. Only Administrators and developers have full access to production data. Administrators and developers require full access to the system and data to write access applications, make changes to the data as required by consistency checks, research data that may be in error to

validate, create apps to store the data in tables and associate all related data pieces, and to test all the listed requirements above. The other personnel listed above under #1 have read access to production data with limitations set by the database views they need access to.

The NRP Risk Assessment determined that the minimum-security class of C2 (Controlled Access Protection) is required for NRP, and that the system will operate in the System High Security Mode. The System High Security Mode requires all users to have the appropriate clearances or authorization, however all users do not have the same need-to-know or access for all the information within the system. Treasury and IRS directives require systems that contain Sensitive But Unclassified (SBU) information to attain C2 security functionality.

NRP stores information protected under the Privacy Act of 1974. Such information is categorized as SBU. In addition, the Commissioner of the IRS has designated that all IRS systems and associated data be categorized as SBU, and protected under IRC 6103, *Confidentiality and Disclosure of Return and Return Information*. Risk Assessments have been performed in accordance with the following guidelines:

- IRM 25.10.1, *Information Technology (IT) Security Policy and Guidance*.
- TD P 71-10, *Security Manual*, October 1, 1992.
- TD P 85-03, *Risk Assessment Guideline*, June 1999.
- CSC-STD-003-85, *Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (TCSEC)*.

Security certification is in progress and is in pending status.

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

NRP uses audit trails as required by IRS IRM 25.10.1, *Information Technology (IT) Security Policy and Guidance*. A Functional Security Coordinator has been assigned. Employees have been trained on the use of the system and their responsibilities concerning access and use of the data. All employees who will work on the NRP have not been determined yet.

The following mandatory rules are defined for users of IRS computer and information systems:

- Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties.
- Users are restricted to accessing, researching, or changing only accounts, files, records, or applications that are required to perform their official duties.
- Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or

financial interest. Users are restricted from accessing the accounts of a famous or public person unless given authorization to do so.

- If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. Users will be held accountable if they access an unauthorized account.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

Sample return data extracted from the RTF, SCRS and TRDB are loaded into the NRP database. For sample returns that are audited, audit results are loaded from the RGS and EOAD systems.

b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?

The Director of the Detroit Computing Center is responsible for protecting the privacy rights of taxpayers and employees regarding data contained within the NRP database. (This section states responsibility for the interface which grants view to the data. As indicated in Section III Attributes of the Data Part 4, the NRP business owner or director is responsible for granting the access provided by and protected by the DCC Director and their staff).

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

External agencies have no access to the system with the exception of the Treasury Inspector General for Tax Administration (TIGTA) and General Accounting Office (GAO) for auditing purposes and only for the amount of time required for the audit. Information within the system will not be disclosed except as expressly authorized by IRC 6103.

b. How will the data be used by the agency?

Not Applicable. No other agencies share data or have access to the data contained in or transmitted by NRP.

c. Who is responsible for assuring proper use of the data?

Not Applicable. No other agencies share data or have access to the data contained in or transmitted by NRP.

d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?

Not Applicable. No other agencies share data or have access to the data contained in or transmitted by NRP.

External agencies have no access to the system with the exception of the Treasury Inspector General for Tax Administration (TIGTA) and General Accounting Office (GAO) for auditing purposes and only for the amount of time required for the audit. Information within the system will not be disclosed except as expressly authorized by IRC 6103.

III. 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 data used in NRP are both relevant and necessary to the purpose for which the system has been designed. The data are needed to produce Service-wide strategic measurements of reporting compliance and provide the ODs with critical information about noncompliant segments of the taxpayer population. IRS also needs the data to update its principal system (DIF) for selecting returns to audit.

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

Yes, the system does derive new data. The derived data is used by analysts for a variety of reasons – to segment the filer population into homogeneous groups, to compare and contrast reporting characteristics, etc. While the derived data have not yet been identified, one example could be “gross profit percentage,” an item not reported on the tax return; but, one that can be derived from reported items – net receipts and gross profit/loss

- b. *Will the new data be placed in the individual’s record (taxpayer or employee)?*

The data is placed in the sample return’s record on the NRP database. No other records (taxpayer or employee) are affected. Returns are classified into 30 Sample Strata. A projected sample size has been determined for each stratum. Returns are randomly selected within a stratum to fulfill the projected sample size. Audit results which result in tax deficiencies are identified and adjusted through the AIMS system as is the current process for making adjustments to the taxpayer’s account by examiners.

- c. *Can the system make determinations about taxpayers or employees that would not be possible without the new data?*

Yes. Determinations about taxpayers will allow us to gain greater insight into the reporting characteristics of noncompliant vs. compliant taxpayers. Determinations about employees that participate in NRP will help us develop better estimates of costs associated with developing and implementing NRP reporting compliance studies. They may also allow us to refine our estimates of the gross income tax gap by analyzing the different skill levels of NRP examiners. The examiners determine the results of the audit based on the data provided in the case and the research performed to detect the extent of non-compliance of

the taxpayer. Therefore, the skill level of the examiner will affect the quality of the audit. The audit results will be the starting point for Research to estimate the gross underreporting gap or gross income tax gap because it indicates the non-compliance rates.

d. How will the new data be verified for relevance and accuracy?

All computer programs written to produce derived data will be thoroughly tested before implementation.

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The NRP host platform protects data by assigning system attributes and resources to pre-defined applications and associated user groups. Users are restricted to those capabilities for which they have been granted permission via the IRS Form 5081. In addition, all IRS personnel receive annual training on the "Taxpayer Browsing Protection Act of 1997" (UNAX) and certify completion of annual UNAX awareness briefing by signature and supervisory acknowledgement.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain

Not Applicable. The NRP system does not consolidate processes.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Although the NRP database contains personally identifiable taxpayer information, it cannot and will not be retrieved by personal identifier by users for research purposes. Only the System Administrator (SA) at DCC has access to this information. The SAs at DCC are also database administrators and developers for the NRP project. The SA only accesses personally identifiable information if needed for error correction or file consolidation in the event of a systemic problem. While the NRP database is being built (from SCRS, TRDB, audit results), authorized users can retrieve data on a specific taxpayer's return with the Taxpayer Identification Number (TIN). The DCC database maintains views to the case data based on user requirements. All identifying taxpayer information is maintained on the database but is not available to users of the database with the exception of the System Administrator at DCC. The user's view to the data for a case is through a generated case number, which associates all data for the case. The actual identity of the taxpayers is not needed. Users with the permission to retrieve data do so using the generated case number or querying on database field values. Regardless of the method a user takes to query a particular case or piece of data, the same view applies to the user, a view where all data contains no taxpayer identifying data such as SSN, name, and address. The NRP Director, only on an individual basis as deemed necessary and appropriate, determines access to

taxpayer identifying data. When the database is complete at DCC, users can retrieve data based on any characteristic or set of characteristics that are maintained in the database. Again, the access and views of the data available to a specific user is based on the user's requirements and approval by NRP management. Characteristics of the data refer to the fields contained in the database, i.e. filing status, total income, etc. These database fields are documented in a data dictionary for the user. Access to this data will be through web-based tools, SQL queries, and report generation applications.

5. *What are the potential effects on the due process rights of taxpayers and employees of:*

a. *consolidation and linkage of files and systems;*

The linkage of files, for example, data from DDB and the taxpayer's return, may reveal potential inaccuracies that an examiner would question. If an adjustment results from this information, the taxpayer is entitled to all due process rights normally allowed in disputes with examiners over proposed adjustments.

b. *derivation of data;*

Derived data will only be used by analysts to identify characteristics (issues and segments) of taxpayers that exhibit reporting noncompliance. This information will then be used to develop/improve programs and treatments to improve compliance with reporting requirements. There is no effect on due process rights of taxpayers or employees. If it results in an audit, the due process provisions of the audit process are put into place. If an adjustment results from this information, the taxpayer is entitled to all due process rights normally allowed in disputes with examiners over proposed adjustments.

c. *accelerated information processing and decision making;*

The accelerated information processing and decision making performed by the NRP system does not affect the due process rights of the taxpayers or employees.

d. *use of new technologies;*

The NRP is not using technologies previously unknown to the IRS.

How are the effects to be mitigated?

Not applicable. NRP is not using technologies previously unknown to the IRS.

IV. Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.

In an effort to ensure equitable taxpayer treatment and avoid overburdening those taxpayers who have been subjected to other types of IRS compliance studies, certain taxpayers were excluded from the NRP. Taxpayers who were selected as part of the 1988 Taxpayer Compliance Measurement Program (TCMP), taxpayers who were selected as part of the Earned Income Tax Credit (EITC) Study and those selected as part of the 1994 Criminal Investigation Study were not selected for the NRP. Those taxpayers selected who were politically sensitive or of a "high profile" nature were treated the same as they are during normal operations audits. Other than those situations above, all sample returns were processed (to the point of return verification) in the same manner.

Case building information (to the extent that it exists) was added to each sample return. Experienced examiners review each sample return and, based on specific criteria and judgment, decide how the accuracy of the return is to be verified, e.g., audited. This determination is enhanced for the NRP examination due to the vast amount of data available to the examiner to make a more accurate and educated judgment. Decisions are reviewed for consistency and reasonableness. Management assists in the development and review of the audit cases. Verification processes are reviewed for adherence to standards, e.g., audit quality. Data is tested to detect input and other errors. All returns were run through the same processes for sample selection, classification and case building therefore ensuring equal treatment of all returns during these processes. Procedures during classification and identifying issues were consistent among all sample-selected returns. Management at classification sites reviewed the quality of the classification and verification processes.

System management is responsible for the proper operation of the system, ensuring correct processing, as well as the oversight of employees' use of the system and the data contained therein

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

NRP is a menu driven application, which provides for consistent use of the system. Training and IRM materials were developed and delivered to personnel involved with (and having responsibilities to interact with) the NRP system. The NRP system applications are accessed from many sites, i.e., CTS (Case Tracking), RGS (Report Generation System), but the applications reside in one location on one system at either DCC or AUCC. Therefore consistent use of the system is enforced by using common menus to an application in one location.

c. Explain any possibility of disparate treatment of individuals or groups.

In terms of the collection of NRP data, IRS requires that some individuals whose returns are sampled by NRP be subject to one of four levels of audit intensity, the lowest being no audit. The determination of which level will be applied is based on sample criteria and an evaluation/review of the sample return. The process has been designed to minimize the intrusiveness of audits and still collect the necessary data. The determination process used in prior years was based solely on the tax return. The determination process for NRP audits differs in that the classifiers and examiners have vast amounts of data available on the taxpayer that gives them the ability to make more educated and accurate decisions on the type of audit intensity, if any, that may be justified.

As far as IRS developing future treatments based on analyses of the NRP data, IRS will seek to develop/update treatments (prefiling, filing, and postfiling) that meet the needs of groups of taxpayers that exhibit common characteristics – notably, problems with reporting income, deductions, taxes and credits. NRP will support the determination of those needs.

2. a. What are the retention periods of data in this system?

NRP uses the same retention schedule as that developed for TCMP. Attachment #2 is the TCMP retention schedule, which is used for NRP.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

Note the attached retention schedule. At the end of the designated retention period, magnetic media will be degaussed, pulverized, and incinerated. These procedures are not documented. The DCC database maintains views to the case data based on user requirements. All identifying taxpayer information is maintained on the database but is not available to users of the database with the exception of the System Administrator at DCC. The user's view to the data for a case is through a generated case number, which associates all data for the case. The NRP Director only on an individual basis as deemed necessary and appropriate determines access to taxpayer identifying data.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

In rare situations, the data may be changed based on analyses and testing that reveal significant error in the original data. For some users, however, data modifications are needed to reflect subsequent year changes in the tax laws. In these instances, the users, e.g., DIF developers create working files from the original NRP data files and make their changes to the working files only. The original data structure and integrity will remain unchanged. These types of modifications to the data require approval from a designated NRP manager prior to access.

3. a. *Is the system using technologies in ways that the IRS has not previously employed (e.g., Caller-ID)?*

No, NRP is not using technologies in ways that the IRS has not previously employed.

b. *How does the use of this technology affect taxpayer/employee privacy?*

Not Applicable. NRP is not using technologies in ways that the IRS has not previously employed.

4. a. *Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.*

No. The system will ultimately produce a data file with all taxpayer identifiers stripped from each record.

b. *Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.*

Yes, in a way; but not the actual taxpayers whose returns are part of the NRP system. Analyses of the NRP data should allow IRS to identify reporting characteristics (issues and taxpayer segments) that need some corrective actions to reduce noncompliance with reporting requirements. IRS programs (prefiling, filing and postfiling) can then be developed based on these analyses. Subsequent NRP studies may then reveal the impact of IRS operational programs to improve compliance with respect to those issues and segments.

c. *What controls will be used to prevent unauthorized monitoring?*

Access to the database has been implemented using roles and views. Database views restrict which fields can be viewed or changed in a given table. Each user is assigned a role. Each role is granted access to only the database views needed to perform their duties.. All employees and contractors receive UNAX and Code of Conduct training. Identification and access provisions are employed.

The DCC database maintains views to the case data based on user requirements. All identifying taxpayer information is maintained on the database but is not available to users of the database with the exception of the System Administrator at DCC. The user's view to the data for a case is through a generated case number, which associates all data for the case. Access to taxpayer identifying data is determined by the NRP Director only on an individual basis as deemed necessary and appropriate. Monitoring of access to data contained in the database is performed using audit trails and audit logs which are reviewed by the SA routinely. (This is not a conflict of interest. The SAs are not users of the data.

They maintain the data. The SAs monitor access by users of the data. All SA activity is monitored through the same channels – audit trails and audit logs. SAs are required to access the system with their own user id which has administrative privileges. Therefore audit trails and logs can identify which SAs performed which functions. The SFC is responsible for monitoring SA activity and misuse.)

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

The applicable SORN for NRP is listed below.

Treasury/IRS No.	System Name
42.021	Compliance Programs and Projects Files – Treasury/IRS

b. If the system is being modified, will the SOR require amendment or revision? Explain.

The SORN identified for NRP will not require amendment or revision. Attachment #3 is the documented proof of analysis and determination by David Silverman that the above SORN is correct.