Federal Trade Commission
Privacy Impact Assessment

for the:

Redress Enforcement Database (RED)

July 2011

1 System Overview

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) enforces many of the nation's consumer protection laws, and works to protect consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace. To further its consumer protection mission, BCP brings law enforcement actions in federal court and in administrative proceedings, and provides consumer and business education to enable the public to avoid common harms.

The Redress Administration Office (RAO) and Division of Enforcement (DE), jointly working with the Office of the Chief Information Officer (OCIO) and with OCIO's contractors, created the Redress and Enforcement Database System (RED). RED collects and maintains information, including personally identifiable information, relating to defendants against whom the FTC has obtained judgments and/or injunctive orders in legal proceedings brought under the FTC Act and other statutes and rules enforced by the FTC. The information enables the Commission to monitor compliance with injunctive orders, collect outstanding judgments, and return the maximum amount possible to victimized consumers.

Division of Enforcement
DE uses the RED to support its mission of enforcing orders obtained in FTC consumer protection actions. The RED collects, secures, and permits authorized FTC staff to review records concerning: defendants who are subject to judgments and/or orders obtained in FTC actions; details of final orders entered as to those defendants; actions undertaken by DE (and other FTC staff, where applicable) in monitoring compliance with those orders; and the status of such compliance monitoring activities. The RED contains related information that furthers DE's order enforcement mission, including contact information for defendants' attorneys, agents, employers, successors, associates, and entities who have facilitated defendants' financial transactions. These entities may possess information about defendants' activities or be required by law to comply with orders issued in FTC actions. (For example, successors may be required to comply with an order as successors-in-interest, and associates and other entities may be required to comply with orders pursuant to Federal Rule of Civil Procedure 65.) DE also uses the RED to maintain contact information for other law enforcement authorities who have expressed an interest in FTC actions, and utilizes the RED as a resource for identifying law enforcement authorities who may also investigate entities bound by orders in FTC actions. Additionally, DE uses the RED to collect and maintain information pertaining to bankruptcy actions initiated by or pertaining to FTC defendants.

Redress Administration
RAO uses the RED to automate oversight of contractors who assist the FTC in administering redress to consumers. The RED tracks court orders that contain a provision for redress, money collected from defendants, debts referred to U.S. Department of Treasury for collection, and cases managed by receivers. RAO enters estimated dollar loss and number of consumers in the RED. RAO collects consumer data, but does not enter any consumer information in the RED. RAO uses the RED to estimate the cost for distributing payments to consumers and/or mailing

consumer education material. If consumer redress is practical, the RED is used to prepare cost estimates, work assignments and approve administrative invoices. The RED stores banking data entered from statements of checking accounts maintained by contractors. This data involves accounts which contain money obtained by the FTC for refunds to consumers, but that data does not contain any personal or identifying information about consumers. The RED also imports financial data from the FTC's Financial Management Office (FMO) accounting system.Finally, the RED also contains contact information and related data regarding receivers appointed in FTC actions, which may be used in identifying potential receivers for future FTC actions.

RED System

The RED utilizes the Oracle Relationship Database Management System to create a secure data repository, and maximize data quality and system performance. The RED is accessible via a secure web-based interface that allows access to the system hosted in the FTC's Data Center. The RED minimizes the manual keying and re-keying of relevant data by having the case managers enter the data via an electronic, web-based questionnaire (E-Survey) instead of on a handwritten form, and by transferring relevant data from existing FTC systems, including the Matter Management System (MMS)[1] and the agency's financial system. The RED maximizes data security by restricting the ability to view the E-Survey for a particular case to a single individual, usually the case manager assigned to that case, and limiting rights to the administrative interface to RAO and DE staff, and other FTC users specifically authorized to access the interface. Users have the ability to read or modify data only if they have been specifically granted such rights for business purposes. While there is some data in the RED that relates to both missions, the interface further maximizes data security by segregating any data relating solely to RAO's mission from data relating solely to DE's mission. Access to either organization's data is provided by that organization only to authorized users with a need to know for official business. User names and passwords are maintained by OCIO in the FTC Oracle system. The RED privileges are maintained within the RED by the RAO and DE administrators.

2 Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

Division of Enforcement

The RED compiles and maintains records relating to defendants who are subject to orders obtained in FTC consumer protection actions; the contents of those orders; actions taken by DE (and other FTC staff, where applicable) in monitoring compliance with those orders; the status of such compliance monitoring activities; law enforcement authorities who have expressed an interest in particular FTC actions; and bankruptcy actions initiated by or pertaining to FTC defendants. No documents are included in the RED, but links to relevant documents on the FTC shared drives are included in the database.

[1]The PIA for MMS can be found at http://www.ftc.gov/os/2007/12/mmspia.pdf.

The personal information collected about defendants includes names, addresses, Social Security numbers (SSNs), dates of birth, employer identification numbers (EINs), home and work phone numbers, email addresses, and contact information for defendants' employers. In addition, the RED includes contact information for defendants' attorneys, agents, successors, associates, and entities who have facilitated defendants' financial transactions; these entities often possess information about defendants' commercial activities and, in certain circumstances, may be required by law to comply with an injunctive order obtained against an FTC defendant.

The information collected for each order includes the date that each judgment or order was entered, the judge and court that entered the order, the parties bound by the order, the statute, products, and alleged violations at issue in the action, the legal basis for any monetary relief in the order, an identification of any bans, bonds, monetary provisions, or suspended judgments imposed under the order, and a statement of whether there is any protective order or centrally-archived paper records pertaining to the case.

The compliance information collected for each order and defendant includes the date that the order was served on each defendant, the date that each defendant delivers to the FTC the acknowledgments of service and compliance reports required by the order, the due dates for compliance reports, a statement of the frequency of order compliance review, the duration of record keeping and compliance monitoring requirements set forth in an order, the status of compliance monitoring activities, and an identification of other persons served with the order. To assist staff in reviewing defendants' compliance with injunctive orders, RED tracks whether defendants have timely submitted required compliance reports and identifies defendants whose compliance monitoring provisions may be expiring.

Information about other law enforcement authorities who have expressed an interest in FTC actions includes those authorities' contact information and summary information regarding criminal actions brought against FTC defendants, including case numbers, indictment dates, conviction dates, and criminal sentences imposed against FTC defendants. The system also identifies defendants who have received a warning letter from the U.S. Food and Drug Administration (FDA).

Bankruptcy information collected for each defendant includes summary information concerning bankruptcy proceedings initiated by or pertaining to FTC defendants.

Redress Administration

The RED tracks broad categories of information concerning redress. For example, the system compiles and maintains information concerning the amount of the judgment debt, the date that the judgment becomes due, payments, and debt delinquency or default. It also contains information regarding the number and total dollar amount of redress distributions, the number of consumers receiving redress, the percentage of loss refunded to consumers, and the fees and costs associated with distributing redress. The RED does not maintain personal information regarding consumers. It does contain contact information and related data concerning receivers appointed in particular cases.

In addition to the redress and enforcement information referenced above, the system logs who enters each item of information (but not who performs queries or views the data).

2.2 What are the sources of the information in the system?

Division of Enforcement
Judgment and order information is entered from court orders. The defendant's personal information is obtained by FTC staff, who obtain such information during the course of investigation and/or order compliance monitoring. Personal information may be collected directly from the individuals and businesses who are the targets of FTC law enforcement actions or from financial statements that defendants may be required to produce. In addition, the FTC may receive personal information in the course of litigation, or in the context of settlement negotiations. The FTC also may obtain information from credit reporting agencies, publicly available databases (such as Lexis/Nexis), or federal, state, or local agencies furnishing identifying information. Information on FDA warning letter recipients is provided by the FDA.

Redress Administration
Consumer loss information is provided by the FTC case manager. The fees and costs associated with distributing redress are defined in the contracts the FTC has with contractors who assist the agency in administering redress to consumers. Consumer information is provided by the defendants or may be collected using claim forms submitted by consumers to contractors which administer redress for the FTC. In some cases, consumer address information may be collected from the U.S. Postal Service or databases such as Lexis/Nexis, but that consumer information is not entered in the RED.

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

Division of Enforcement
DE collects the above information to maintain records about individuals who are named in orders obtained by the agency, who may be subject to such orders, or who owe money to the FTC, so that the FTC may monitor compliance with and enforce existing judgments and injunctive orders, and report on its activities. Data elements such as SSN and date of birth are necessary to accurately monitor defendants, confirm that individual defendants are correctly identified, and to ensure that any communication with the Department of Treasury identifies the correct individual.

The FTC also collects address information for defendants' successors, associates, and financial entities that facilitate defendants' transactions, in order to maintain a record of persons or entities who may have information about the defendants' commercial activities or who may be required by law (pursuant to Federal Rule of Civil Procedure 65 or otherwise) to comply with an order obtained by the FTC.

DE collects contact information of other law enforcement authorities to facilitate communication

with those authorities and identify law enforcement authorities who may also investigate entities bound by orders in FTC actions. Information on FDA warning letter recipients is cross-checked against FTC defendants to identify whether any FTC defendants have received FDA advisories that may relate to their compliance with an order obtained by the FTC.

DE collects summary information about bankruptcy proceedings relating to FTC defendants to assist its staff of bankruptcy specialists who advise other FTC staff with respect to such proceedings.

Redress Administration
RAO uses the RED to track defendant information, not PII consumer information. RAO uses defendant information to facilitate the collection and resolution of debts.

The other type of information in RED is related to case management. This information includes billing units and fees related to FTC's contracts with contractors who assist in administering redress. This data is used in cost estimating, issuing work assignments, and approving redress contractor invoices. The RED tracks milestones and case notes to measure RAO performance compared to the Government Performance and Results Act.

RAO uses the RED to collect data for other offices. RAO enters receivership contact information for use by FMO. FMO mails surveys to receivers to track financial activity. RAO collects estimates on collectibility of defendants' debts from case managers so FMO can record allowance for uncollectible accounts. RAO also tracks total dollars and checks issued by country within each matter. RAO provides data involving checks issued to consumers in foreign countries ("Foreign Claimant data") to the FTC's Office of International Affairs; this includes the matter number, the foreign country, and the sum total in dollar amount paid out in that country (but not information about the individuals to whom redress was paid). Active bank account information is provided to the FTC's Office of Inspector General for confirmation letters as part of the annual audit of redress funds.

2.4 How is the information collected?

Division of Enforcement
Information is collected by FTC case managers who review the legal documents associated with a case and enter that information into the RED. The case managers enter the data via an electronic, web-based questionnaire (E-Survey) made available via the FTC's intranet, instead of using a paper form. DE staff also input information into the RED in the course of monitoring defendants' compliance with final orders. In addition, data is entered by transferring relevant data from the FTC's Matter Management System and inputting warning letter data received from FDA.

Redress Administration
Estimates on collectibility of debt are collected by sending E-Surveys to case managers. RAO enters U.S. Department of Treasury referrals using information provided by FTC case managers at the time the case is referred to RAO. RAO enters data from the FTC contracts between the

FTC and redress contractors. Redress banking and checking data (including matter name and bank name, but no information about individual consumers) is entered by RAO from bank statements. Financial data from FMO is imported from the agency's financial system. Case management data is entered by RAO from discussions with case managers. Foreign Claimant data is provided by redress contractors and entered by RAO. Receiver data is entered using information from court orders and E-Surveys completed by FTC case managers.

2.5 How will the information be checked for accuracy and timeliness (currency)?

When the case managers reply to an E-Survey, the information is reviewed by DE and/or RAO administrators, supervisors, and/or program staff. If the data is complete, it is entered into the RED. If information from an E-Survey is rejected, DE or RAO staff contacts the case manager to correct the deficiency. DE staff assigned to monitor defendants' order compliance review check data for accuracy and currency. RAO enters case management data daily as the status of the case changes. The case status reports are discussed with redress contractors monthly to check accuracy and plan redress activity. Data from MMS is imported daily. FDA data is imported on a monthly basis. FMO data is imported when RAO notifies OCIO to load data, which can be daily but is collected at least on a monthly basis. RAO reconciles financial data from FMO and bank statements monthly. U.S. Department of Treasury referral data is verified at time of entry and updated quarterly. Collectibility of debts, receiver data, and Foreign Claimant data is checked by RAO annually.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

No. The system uses technologies only in ways which the Commission has previously employed. The RED utilizes a database and a set of tools provided by Oracle Corporation to manage the data, security, and business rules of the application. Using this Oracle system maximizes data quality, data security, and system performance. Users access the RED using a web-based application that is only accessed within the FTC's intranet.

2.7 What law or regulation permits the collection of this information?

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, authorizes the FTC to collect and store this information.

In addition, pursuant to a Memorandum of Understanding (MOU) prepared in connection with the Debt Collection Improvements Act of 1996 (DCIA), 31 U.S.C. § 3720B - 3720E, the FTC must send eligible judgments no longer being litigated that have been outstanding and delinquent

for 180 days or more to the U.S. Department of Treasury for collection. The Treasury requires the FTC to provide each judgment debtors' name and SSN or EIN. The FTC must collect SSNs and EINs in connection with tax reporting requirements for judgment defendants. 31 U.S.C. § 7701. If a debt referred to Treasury is not collectible, Treasury may issue 1099-C forms to each defendant who has not paid an outstanding judgment in full.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The system is used only for internal purposes (subject to the information in Section 3.3 below), and the FTC maintains safeguards to protect this information as described below. Risks to privacy arise primarily from internal threats to the information contained within the RED database, which include the unauthorized or inadvertent release of PII and unauthorized browsing for information. Several safeguards have been implemented to mitigate these risks, and to prevent the unauthorized disclosure of PII from the RED.

First, only FTC staff and contractors with an OCIO issued user-identification and password, which must be a strong password, can access the system. The RED administrators in DE and RAO limit the ability to view, add, change, or delete information by setting user roles within the RED. The RED maximizes data security by restricting the ability to view the E-Survey for a particular case to a single individual, usually the case manager assigned to that case. These restrictions help to protect the information in the RED from internal threats.

Second, the server on which the database is stored is protected by a firewall and is not accessible from outside the Commission.

Third, the RED interface further maximizes data security by segregating any data relating solely to RAO's mission from data relating solely to DE's mission. Access to either organization's data is provided by that organization only to authorized users with a need to know for official business.

Finally, there is inherent in any data collection the risk of over collection, or collecting more data than is necessary to accomplish the purposes of the system. The FTC strives ro collect information only where there is a legitimate need to do so. Staff and the Chief Privacy Officer have reviewed the data elements and determined that each is necessary and must be collected to effectively implement our redress and enforcement programs.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

The FTC will use information in the RED to administer its order compliance monitoring and enforcement activities and to collect monies from defendants who have defrauded or otherwise victimized consumers and who have been prosecuted through an FTC law enforcement action. The FTC may also use the information about defendants, and their agents, successors, and associates, for internal reporting purposes, to pursue corollary investigations, to meet tax reporting obligations, and for other uses authorized by existing System of Records Notices (SORNs). See *infra* Section 8. The FTC will use the contact information of receivers to identify parties who can assist the FTC and the court in cases where defendants' assets are to be frozen, marshaled, or liquidated. The FTC will use the contact information of law enforcement personnel to identify and contact those authorities with respect to FTC actions.

3.2 Which internal entities will have access to the information?

The RED may be accessed by case managers, RAO and DE staff, and other authorized FTC staff in BCP or the FTC's Regional Offices. Users authorized to access the RAO data maintained in the system use a separate interface than that employed by users authorized to access DE data, in order to limit access to each organization's data. Technologists in OCIO can upload information from MMS and the FMO accounting system, as well as correct data at the direction of RAO/DE administrators. In addition, data may be sent to the OIG for internal audits.

3.3 Which external entities will have access to the information?

No external entities have direct access to the information. RAO or DE may provide data or reports from the RED to external entities as described below.

RED Software Contractors
OCIO contractors may be authorized to access data in the RED to perform technical work relating to the development and maintenance of the system. The OCIO contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the agency.

Redress Contractors
The RED contract data is used to prepare work assignments which RAO sends to redress contractors. The RED contract data is also used to review administrative and tax invoices from

redress contractors. RAO sends consumer information to redress contractors, but no consumer information is entered into the RED.

The U.S. Department of Treasury
RAO discloses defendant data collected in the RED to the U.S. Department of Treasury when it refers eligible defendants to that agency for further collection of judgments. The U.S. Department of Treasury may share this information with the U.S. Department of Justice or any of the private collection agencies that may be assigned the FTC debt for collection. These disclosures are appropriate because monies ultimately collected by U.S. Department of Treasury, DOJ, or private collection agencies will be used (if appropriate) for consumer redress. If a debt proves to be uncollectible, U.S. Department of Treasury may then issue 1099-C forms to each defendant who has not paid a judgment in full.

External Law Enforcement
The FTC may disclose information in the RED with other federal, state, local, or international law enforcement agencies in the course of a law enforcement investigation or action.

Other Disclosures
The FTC may be required or authorized to share certain data collected in the RED in other circumstances, including in response to requests from Congress, Freedom of Information Act (FOIA) requests from private individuals or entities, requests from the media (not obtained through a FOIA request), or during litigation. In these situations, the FTC redacts personal identifying information pursuant to agency policy and any applicable rules or orders of court before providing data.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

To the extent the FTC attempts to collect information directly from defendants and related persons or entities through investigation, litigation, or voluntary settlement negotiations, these persons or entities have notice of the FTC's efforts and opportunity to decline cooperation or to assert a privilege or immunity from providing this information. In the context of voluntary settlement negotiations, the FTC may request that defendants provide such information under penalty of perjury in a personal financial statement. FTC final judgments resulting from negotiated settlements often contain standard language, similar to the following, informing defendants that the information may be used for collection:

In accordance with 31 U.S.C. § 7701, Defendants are hereby required, unless they have done so already, to furnish to the Commission their respective taxpayer identifying numbers (social security numbers or employer identification numbers) which shall be used for purposes of collecting and reporting on any delinquent amount arising out of Defendants' relationship with the government.

Defendants indicate their consent to the collection and use of their information by signing the final judgment.

To the extent the FTC obtains personal information concerning defendants and related persons or entities from third parties and other sources, such as other law enforcement agencies or private credit reporting agencies, or public sources, such persons and entities may not have notice or an opportunity to consent to the collection or use of the information.

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

Individuals that provide the FTC with information on a voluntary basis may choose to decline to provide such information. However, individuals do not have a right to decline to provide information that is required by law and/or court order.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals generally do not have a right to consent to particular uses of the information stored in the system. An exception is in FTC administrative or court proceedings, where individuals may in some cases limit the agency's use or disclosure of their information that may be stored in the system (e.g., under a stipulated pre-trial protective order or other binding agreement in discovery).

4.4 What are the procedures that allow individuals to gain access to their own information?

Consumers, individual defendants, and others (e.g., law enforcement contacts) whose information may be contained in the RED database do not have access to the database. Individuals seeking access to such records must file written request under the Freedom of Information Act (FOIA), 5 U.S.C. 552, with the FTC's Office of General Counsel. *See* Rule 4.11(a), 16 C.F.R. 4.11(a). Any additional request for mandatory access under the Privacy Act of 1974, 5 U.S.C. 552a, must also be made in writing to the General Counsel, and may be filed only by an individual for records, if any, retrieved by that individual's name or other personally assigned identifier. *See* Commission Rule 4.13, 16 C.F.R. 4.13. Due to the law enforcement nature of RED database, the General Counsel may deny access to records that are legally exempt from disclosure. See 16 C.F.R. 4.10(a) (nonpublic materials not subject to FOIA disclosure), 4.13(m) (Privacy Act exemptions). For information on how to file a FOIA or Privacy Act request, please visit the Commission's FOIA Web page, located at http://www.ftc.gov/foia/contact.shtm.

Apart from the Privacy Act, once an FTC investigation is concluded, individuals (e.g., investigatory targets) who have provided materials under compulsory process or voluntarily during the investigation may make a written request to FTC staff for the return of any such materials, excluding materials that the FTC is entitled or required by law to withhold or preserve.

See 15 U.S.C. 57b-2 (FTC Act), 16 C.F.R. 4.12 (FTC Rules of Practice).

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

There are no privacy risks associated with access to the RED system because individuals do not have access to it. Individuals seeking the RED records about themselves may only access their records as described in Section 4.4. The Commission's Privacy Act procedures permit the FTC to verify a requesting individual's identity before granting him or her access to the records at issue.

5 Web Site Privacy Issues

The RED cannot be accessed or disclosed through any public or private website. Therefore, this section is not applicable.

6 Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The RED is a part of the FTC's Data Center General Support System (Data Center GSS).[2] The FTC follows all applicable Federal Information Security Management (FISMA) requirements, ensuring the Data Center GSS is appropriately secured. The Data Center GSS is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

A Certification & Accreditation for the Data Center GSS, which includes the RED, is in process.

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed for the Data Center GSS, which includes the RED.

[2]The Data Center GSS PIA is available here: http://www.ftc.gov/os/2011/08/1108datacenter.pdf

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No.

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

Supervisors and/or Contracting Officer's Technical Representatives (COTRs) must identify and approve employee requests to access RED and specify the appropriate access privileges. RED access is based on least-privilege and need-to-know security models.

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

All FTC staff are required to complete computer security and privacy awareness training annually. Interactive online training covers topics such as proper handling of sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

Auditing measures and technical safeguards are in place commensurate with the National Institute for Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 3.

6.8 Where should questions regarding the security of the system be directed?

Any questions regarding the security of the system should be directed to the FTC's Information Assurance Manager.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

The FTC has submitted to the National Archives and Records Administration (NARA) a comprehensive records disposition schedule, SF-115 Request for Disposition Authority. Pending NARA approval, FTC will manage usage information in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 C.F.R. Ch. XII, Subchapter B, Records Management, and OMB Circular A-130, par. 8a1(j) and (k) and 8a4. FTC has proposed a retention period of six years for each redress class member data set upon the close of Commission redress action or when no longer needed for legal and FTC business purposes, whichever is sooner.

7.2 What are the plans for destruction or disposal of the information?

All information that is subject to disposal (see Section 7.1) will be destroyed in accordance with OMB, NIST, and NARA guidelines.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

The FTC recognizes that there could be privacy risks associated with the disclosure of addresses, telephone numbers and facsimile numbers in the RED. These include the defendants' personal and employer addresses, receivers' business addresses, criminal law enforcement contacts' business addresses, and successors' and related person's addresses. Such information is available to anyone with read-only access to the system. However, the level of protection for this information is consistent with data protections afforded for similar information by other data systems maintained by the FTC, notably the MMS and Consumer Information System (CIS). Moreover, unlike CIS, access to the RED will be limited to FTC employees and contractors, who are bound by the FTC's Privacy Policy. Access to the RED is restricted to authorized users within RAO and DE, selected employees in the FTC's Bureau of Consumer Protection and its Regional Offices, and authorized FTC contractors performing work specifically relating to the database.

The FTC also assessed the system's "E-survey" web form for privacy risks associated with the use of persistent tracking technology, such as permanent "cookies" or other permanently placed software files or other information on user's computers. Because the web form activated by the "E-survey" does not use such persistent tracking technology, no such privacy risks are raised.

8 Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

Yes.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes. The applicable Privacy Act SORN is FTC I-1, which describes the FTC's Nonpublic Investigational and Other Nonpublic Legal Records, including enforcement-related data maintained by the FTC in RED, as described above. The SORN is posted on the FTC's web site and can be found at http://www.ftc.gov/foia/sysnot/i-1.pdf.

9 Privacy Policy

The collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's Privacy Policy.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
David M. Torok, Associate Director
Bureau of Consumer Protection
Division of Planning and Information

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Marc Groman
Chief Privacy Officer

_____ Date: _____
Margaret Mech
Chief Information Security Officer

_____ Date: _____
Jeffrey Nakrin
Records Officer

Approved:

_____ Date: _____
Jeffrey Huskey
Chief Information Officer