Animal and Plant Health Inspection Service (APHIS)
Marketing & Regulatory Programs Business Services (MRPBS)

AUTOMATED TRUST FUNDS DATABASE

PRIVACY IMPACT ASSESSMENT (PIA)

FINAL

October 25, 2007

Prepared For:

USDA
Animal and Plant Health Inspection Service
1400 Independence Avenue, S.W.
Washington, DC 20250

Prepared By:

9140 Guilford Road, Suite N
Columbia, MD 21046

FOR OFFICIAL USE ONLY

Name of Project: Automated Trust Funds Database Minor Application
Program Office: Animal and Plant Health Inspection (APHIS), Marketing & Regulatory Programs Business Services (MRPBS)
Project's Unique ID: 005-32-01-01-02-3001-00-402-124-1499-12

A. CONTACT INFORMATION:

1. Who is the person completing this document?
Name: COACT, Inc.
Position Title : Contractor
Program Area: MRPBS
Telephone Number **: 301-498-0150**

2. **Who is the system owner?**
Name: Vikki Soukup
Position Title: Program Manager/Supervisory Accountant
Program Area: MRPBS/FMD
Telephone Number: 612-336-3237

3. Who is the system manager for this system or application?
Name: Vikki Soukup
Position Title: Program Manager/Supervisory Accountant
Program Area: MRPBS/FMD
Telephone Number**: 612-336-3237**

4. Who is the IT Security Manager who reviewed this document?
Name: Billy Smith
Position Title: ISSPM
Program Area: MRPBS
Telephone Number**: 301-734-7604**

5. Did the Chief FOI/PA review this document? (Name, office, and contact information).
Yes.
Tammi Hines
Freedom of Information & Privacy Act Staff
(301) 734-8296

6. Did the Agency's Senior Office for Privacy review this document? Name, office, and contact information).
Yes.

Tammi Hines
Freedom of Information & Privacy Act Staff
(301) 734-8296

7. **Who is the Reviewing Official?** (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

   Gregory Parham
   Chief Information Officer
   MRPBS Information Technology Division
   (301) 734-5328

USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: Automated Trust Funds Database Minor Application

Description of Your Program/Project: The Automated Trust Funds Database is a client based minor application that uses financial data extracted directly from the USDA Financial Data Warehouse (FDW) to generate monthly customer account statements. These statements are distributed to field offices to address cooperator queries and concerns as well as provide status of trust fund accounts. Cooperators are foreign organizations seeking trade with the U.S. They typically reside in countries that have processing standards that do not meet existing U.S. guidelines. Therefore the USDA performs inspection and other services for cooperators to ensure that cooperator products being brought into the U.S. are safe for consumption or use.

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system.	The Automated Trust Funds Database is an accounting system that extracts data directly from the USDA FDW to produce monthly trust fund account statements. The information in the system reflects trust fund status to include expenditures, overhead and collections based on inspection trust fund credits, costs and services.
2a. What are the sources of the information in the system?	Information is extracted from the USDA FDW.
2b. What USDA files and databases are used? What is the source agency?	Only the USDA FDW database is used.
2c. What Federal Agencies are providing data for use in the system?	Information is only derived from USDA systems.
2d. What State and Local Agencies are providing data for use in the system?	State and Local Agencies do not provide data for use in the system.
2e. From what other third party sources will data be collected?	Data is not collected from third-party sources.
2f. What information will be collected from the customer?	Data is not collected from the customer. The system extracts information such as Cooperator Name, system account number, address, country, previous month's balance, collections, expenses, and refunds from the FDW. Information from Brio reports are used to validate account balances and post information from Detailed Transaction Reports to the statements being queried. Information from the FDW may be used during cooperator record creation and update or to update or create contact list information.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Data is only collected from USDA sources. Brio reports and reports from the Central Accounting System (CAS) are used to validate the accuracy of information within the trust statements.

3b. How will data be checked for completeness?	The ATF is basically an information extraction process pulling information from the FDW. Information is reviewed for completeness and in those cases where there are discrepancies, Brio and CAS reports are used for validation checks. Errors are reconciled and reconciliation reports are produced to clarify discrepancies. In the event that there are debt inconsistencies, this information will be reported to the Debt Management Team.

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	System access is limited to approximately 4 general users within the APHIS MRPBS Financial Management Division to include the system manager and system administrators troubleshooting application problems, performing maintenance or other system administrative functions. Only one user can access the system at any given time. The system also requires identification and authentication.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Application access is determined by user role and is given on a need-to-know basis. Only a limited number of users can access the system and only one user at a time. System administrative personnel install the client software, which is needed for access, on those systems within the Financial Management Division that are authorized by the system owner to access this data.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	Users will have access only to that data required to fulfill their functional or operational role. The application is developed to only extract information from resources necessary to develop the monthly account statements. This information originates from the FDW. Users must log in and select the fiscal month and fiscal year for statements that require retrieval and distribution. If retrieval has been performed, the process is only executed when overhead or some other discrepancy is noted from review of other reports.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	Only one user can be logged into the system at any given time. Access to the application is limited and requires install of client software for access. Downloaded files are stored in portable document format (PDF) and stored on a file server. Access to the files on the file server is restricted to those persons authorized to distribute trust fund files.
5a. Do other systems share data or have access to data in this system? If yes, explain.	The ATF Database does not share data. Information from the application is used in monthly reports to update information in the Foundation Financial Information System (FFIS).

5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	The ATF system owner, and system support personnel will be accountable for covering any perceived gaps in protecting privacy rights. This includes risk and privacy assessments, vulnerability identification, and handling disclosures issues.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	Only authorized USDA officials and employees will have access to the data. Data is not shared with International, Federal, State, Local, or other agencies.
6b. How will the data be used by the agency?	The agency will use data to provide field offices with monthly account statements reflecting trust fund account status associated with USDA inspection services.
6c. Who is responsible for assuring proper use of the data?	The system owner, and system support personnel are responsible for assuring that data is properly used and protected from unauthorized disclosure. The system will be protected using role based access control for the users and system administration personnel. Also, all APHIS personnel is required to take the security awareness training.

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 within the application is used to provide field offices with trust fund account status so that they can respond to queries by cooperators. These trust funds hold monies that are collected in advance of inspection services, with monthly statements providing details of costs associated with these services.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No. The Automated Trust Fund Database does not create data previously unavailable about an individual. Most of the information is simply imported from other accounting sources to produce the trust funds statement.
2b. Will the new data be placed in the individual's record (customer or employee)?	No. New data will not be created or placed in an individual's record, unless it is inserted to update the status of a record or correct information such as address and phone number.
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	The system can not make determinations about customers or employees.
2d. How will the new data be verified for relevance and accuracy?	Users will perform calculations and review data using Brio query reports to identify spending and overhead discrepancies. Reconciliation reports or debt management processes will be conducted to resolve discrepancies.

3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	Data extraction is limited to a small group of users with only this group of individuals having access to the data in this system. Prior to accessing application data, users must also authenticate using network provided unique system identification and passwords. In addition, each system using the application must have application software properly installed and configured on their system.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Domain controls from network services control and limit access to files on the share drive and to those downloaded to the local workstations.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Yes. Data will be retrieved by making a query for a batch of statements for a given month. Retrieval is performed only once a month. Queries can be made based on trust fund identification numbers or trust fund names as part of the trust fund forms maintenance operations. While the typical process is to make queries from the system using dates and identification numbers, some queries are possible from the Administrative Info Maintenance Form sections of the application. These queries can be performed on fields such as address, city, state, zip code, or country. Fields such as the address section may be personally identifiable to an individual.
4b. What are the potential effects on the due process rights of customers: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	There are no potential effects on the due process rights of the customer. The system is a benefit for the customer as it allows production of monthly account statements reflecting trust fund status and this information is used to calculate overhead based on actual charges or identify debt. This information is released to field offices that respond to cooperator queries.
4c. How are the effects to be mitigated?	There are no effects to be mitigated.

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers.	The information dispersed by the system is done once a month for all customers. System users perform retrievals based on dates, not individual characteristics.
2a. 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 system is not operated in more than one site and consistency is maintained by allowing only one user access at a time.
2b. Explain any possibility of disparate treatment of individuals or groups.	The ATF Database presents no potential for disparate treatment of individuals or groups. Data retrieval is performed based on date and company information with a separation between the customer, who interacts with field offices, and the system users, who correspond with the field offices.
2c. What are the retention periods of data in this system?	Online data is indefinitely maintained in the database and on the file server. This is in accordance with the National Archives and Record Administration (NARA) guidelines.

2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Since the systems inception, the Accounting and Payment Team has created monthly folders for each Fiscal Year to store data. Procedures defining a retention period and processes for eliminating data will be documented. Appropriate team members are already discussing the requirements.
2e. 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?	Data is stored in PDF files and does not require modification. No determinations are made on the data being stored. Files are also stamped with the creation date in the lower left hand corner of the statement. Data is also stored on a network file server which has numerous inherent safeguards to protect the data such as: • Required login and authentication for network access • Domain access enforced at login by the Microsoft Windows 2003 Server • Role based access controls enforced by the Active Directory Group Policy
3a. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?	No, the system is not using technologies in ways not previously employed by the agency.
3b. How does the use of this technology affect customer privacy?	The technology used within the ATF does not impact customer privacy.
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	The system does identify individuals within a contact list. This information may consist of location, phone number and mailing address to resolve discrepancies related to trust funds accounts. However, there is no live monitoring of individuals.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	The system does identify companies by name, address, and phone numbers, but only to produce trust fund statements for active accounts. Similar to the prior response, groups or corporate entities are identified and are susceptible to scams and social engineering attempt. However, safeguards are in place to reduce the risks associated with such events such as proper handling of data, background checks for personnel, and access control.
4c. What controls will be used to prevent unauthorized monitoring?	Monitoring is not a feature of the application; however, the application is configured to allow use by a single user. The number of users accessing the data is limited. In addition, administrators of the network performed auditing and all employees must consent to being monitored for access.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name. (SORs can be viewed at www.access.GPO.gov)	There is currently no SOR for the ATF Database. MRPBS will develop a plan of action & milestones (POAM) to address the issue of developing an SOR.

5b. If the system is being modified, will the SOR require amendment or revision? Explain.	N/A