

FOR OFFICIAL USE ONLY



Committed to the future of rural communities.

Privacy Impact Assessment

For

Business Intelligence

HYPERION PERFORMANCE SUITE

ELECTROFICHE

FOCUS/WEBFOCUS

TABULAR DATA WAREHOUSE

Version 1.0

April 2007

FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Business Intelligence System. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

The document is accepted.

The document is accepted pending the changes noted.

The document is not accepted.

_____ We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

System Manager - Marilyn Miller

5/25/07
DATE

OCIO/Project Representative – Eugene Texter

5-25-07
DATE

Program/Office Head - Peggy Stroud

6/6/07
DATE

OCIO – John Distler

6/6/07
DATE

Chief FOI/PA – Brenda Dinges

6/28/07
DATE

Senior Official for Privacy - Christopher L. Smith

6/6/07
DATE



FOR OFFICIAL USE ONLY

Table of contents

A. CONTACT INFORMATION..... 1

B. SYSTEM APPLICATION/GENERAL INFORMATION 3

C. DATA IN THE SYSTEM 5

D. ATTRIBUTES OF THE DATA..... 9

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS 11

F. ACCESS TO THE DATA 13

APPENDIX A 17

APPENDIX B 19

POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS 19

FOR OFFICIAL USE ONLY

Name of Project: Business Intelligence
Program Office: Rural Development
Project's Unique ID: BI

Information System Name/Title	Business Intelligence
System Acronym	Business Intelligence
System of Records (SOR)	USDA / RD-SOR-1
System Type	<input type="checkbox"/> GSS <input checked="" type="checkbox"/> MA <input type="checkbox"/> GSS sub-system <input type="checkbox"/> MA individual application
Responsible Organization	USDA – Rural Development

A. CONTACT INFORMATION

1. Who is the person completing this document? (TDW)

Name	Susie Maxwell
Title	IT Specialist, Team Leader
Address+	USDA RD 1520 Market Street St. Louis, MO 63103
Email address	Susie.maxwell@stl.usda.gov
Phone Number	(314) 335-8601

(Hyperion)

Name	Gayle Doss Dwana Davis
Title	Systems Analyst/IT Specialist
Address	USDA RD 1520 Market Street St. Louis, MO 63103
Email address	Gayle.doss@stl.usda.gov Dwana.Davis@stl.usda.gov
Phone Number	(314) 335-8622 (314) 335-8716

(FOCUS/WebFOCUS)

Name	Julia Cole
Title	IT Specialist (Data Management)
Address	DCIO/Technical Support & Standards Compliance Division Data Management Services Branch 1520 Market Street, FC-432 Saint Louis, MO 63103
Email address	julia.cole@stl.usda.gov



FOR OFFICIAL USE ONLY

Phone Number	314-335-8734
---------------------	--------------

(Electrofiche)

Name	Susie Maxwell
Title	IT Specialist, Team Leader
Address	USDA RD 1520 Market Street St. Louis, MO 63103
Email address	Susie.maxwell@stl.usda.gov
Phone Number	(314) 335-8601

2. Who is the system owner?

Name	Peggy Stroud
Title	Director, Systems Design and Development Division
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	Peggy.stroud@stl.usda.gov
Phone Number	314-335-8925

3. Who is the system manager for this system or application?

Name	Marilyn Miller
Title	Director, Technical Support and Standards Compliance Division
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	Marilyn.miller@stl.usda.gov
Phone Number	(314)-335-8123

4. Who is the IT Security Manager who reviewed this document?

Designated Approval Authority	Eugene Texter
Title	Information Security Staff Team Lead
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	eugene.texter@stl.usda.gov
Phone Number	(314)-335-8104

5. Did the Chief FOI/PA review this document?

Name	Brenda Dinges
Title	Information System Security Program Manager
Address	USDA Rural Development



FOR OFFICIAL USE ONLY

	1520 Market Street St. Louis, MO 63103
Email address	brenda.dinges@stl.usda.gov
Phone Number	(314)-335-8829

6. Did the Agency's Senior Office for Privacy review this document?

Name	Christopher L. Smith
Title	Rural Development CIO
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	(202)-692-0212

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).

Name	Christopher L. Smith
Title	Rural Development CIO
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	(202)-692-0212

B. SYSTEM APPLICATION/GENERAL INFORMATION

Business Intelligence is a combination system comprised of applications Hyperion (Brio), Electrofiche, FOCUS, and Data Warehouse. It is a mission-critical system with a FIPS 199 security rating of "moderate."

HYPERION is a commercial off the shelf (COTS) application server that provides query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology for centralized connectivity to a variety of data sources.

ELECTROFICHE is a medium to store, read and retain files for USDA. These files are reports generated by USDA enterprise-level accounting and reporting systems. Customer access to this media is browser based. Electrofiche is available for Large Office and Field Office access.

FOCUS is utilized in producing reports from data residing on the National Information Technology Center (NITC) mainframe located in Kansas City, Missouri. FOCUS is capable of providing a complete information control system with comprehensive features for entering, maintaining, retrieving, and analyzing data. RD mainly utilizes the end-user reporting features of the FOCUS software.



FOR OFFICIAL USE ONLY

TABULAR DATA WAREHOUSE: The establishment of RD Data Warehouse began in 1999. The Data Warehouse provides critical business data, for RD decision-makers to sustain their respective program missions. Information is available to ensure loans and grants are optimally provided in the areas where the need is greatest, and correspondingly stimulates growth and job creation.

<p>1. Does this system contain any information about individuals?</p>	<p>Electrofiche, FOCUS/WebFOCUS: Yes Hyperion: The System contains the eAuthentication internal id and user name for individuals. This information is used to authorize access to content and role-based functions within the application. The application administrator has configured the system to maintain usage records that identify system login and document retrieval information. TDW: Customer demographics and information related to loan making and loan servicing activities from the various on-line transactional processing (OLTP) systems/subsystems; including Guaranteed Loan System (GLS), a Guaranteed subsystem; Direct Loan Origination and Servicing (DLOS) which consists of MortgageServ and UniFi; Multi-Family Management (MFM); Water and Environmental Programs (WEP), a Guaranteed component; Guaranteed Underwriting System (GUS), a Guaranteed component; Water and Environmental Programs (WEP), which includes Community Programs Application Processing (CPAP); and Rural Utility Loan Servicing System (RULSS), is contained within the TDW. The TDW also provides restricted access to human resources data, which includes employee demographics and data related to pay, work performance, etc.</p>
<p>(a) Is this information identifiable to the individual? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, <u>the remainder of the Privacy Impact Assessment does not have to be completed past this section.</u></p>	<p>Electrofiche, FOCUS/WebFOCUS, TDW: Yes Hyperion: Yes, user eAuthentication internal ids and full names are stored in the application. The usage records can be mapped to the user.</p>
<p>(b) Is the information about individual members of the public?</p>	<p>Electrofiche, FOCUS/WebFOCUS: Yes Hyperion, TDW: No</p>
<p>(c) Is the information about employees?</p>	<p>Electrofiche: No FOCUS/WebFOCUS, Hyperion: Yes TDW: Yes, As noted in response to question 1 above,</p>



FOR OFFICIAL USE ONLY

	<p>the TDW provides restricted access to human resources data, which includes employee demographics and data related to pay, work performance, etc.</p>
<p>2. What is the purpose of the system/application?</p>	<p>FOCUS/WebFOCUS: FOCUS is capable of providing a complete information control system with comprehensive features for entering, maintaining, retrieving, and analyzing data. Its main purpose is to provide reporting capabilities. Electrofiche is a medium to store, read and retain files for Rural Development and Farm Services Agency. These files are reports generated by USDA enterprise-level accounting systems. HYPERION is a Commercial Off-the-Shelf (COTS) application server that provides query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology for centralized connectivity to a variety of data sources. TDW: The Data Warehouse provides personnel from the RD major program areas with information needed to make sound management decisions that efficiently and effectively support the needs of their customers.</p>
<p>3. What legal authority authorizes the purchase or development of this system/application?</p>	<p>FOCUS/WebFOCUS: NITC provides FOCUS/WebFOCUS for use by multiple agencies. Electrofiche: The Paperwork Reduction Act of 1995 – to ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government. Hyperion: USDA Rural Development TDW: The establishment and development of the tabular data warehouse resulted from the joint efforts of a Service Center Initiative Team comprised of RD, FSA and NRCS. Establishment and development of the TDW was sanctioned and approved by OCIO.</p>

C. DATA in the SYSTEM

<p>1. Generally describe the type of information to be used in the system and what categories of individuals are covered in the system?</p>	<p>FOCUS/WebFOCUS: <u>Borrower information:</u> name, address, SSN, statistical data and loan & grant information are provided. <u>Employee information:</u> Only Rural Development, Farm Service Agency and Office of the Inspector General employees have access. User names, User IDs, and passwords are encrypted. Electrofiche Customer: Rural Development – Information used depends on the report requested and</p>
---	---

FOR OFFICIAL USE ONLY

	<p>its enterprise system source.</p> <p>HYPERION System Information: eAuthentication id, application files (.bqy), .bqy file directory locations, .bqy file descriptions, .bqy file display names, user to group mappings, application job scheduling events, job schedules, job actions, and usage records.</p> <p>HYPERION Employee Information: eAuthentication internal id, user names, organization code, used for authorizing access to content when accessing the system.</p> <p>TDW Customer Information: Customer demographics and information related to loan making and loan servicing activities from the various OLTP systems, including Guaranteed Loan System (GLS), Direct Loan Origination System (DLOS), Multi-Family Management (MFM), Water and Environmental Programs (WEP), which includes Community Programs Application Processing (CPAP), Guaranteed Underwriting System (GUS), and Rural Utility Loan Servicing System (RULSS).</p> <p>TDW Employee Information: Restricted access to human resources data from National Finance Center (NFC), which includes employee demographics and data related to pay, work performance, etc.</p> <p>TDW Other Information: Transactional data from the Program Funds Control System (PFCS) and Program Loan Origination and Servicing System (PLAS) an FSA owned system, supported and shared usage by RD.</p>
<p>2. What are the sources of the information in the system?</p>	<p>FOCUS/WebFOCUS: RD and FSA loan and grant account information stored on the NITC mainframe. EPA hazardous site information</p> <p>Electrofiche Customer: Enterprise-level system reports including PLAS, AMAS, GLS, and PFCS.</p> <p>HYPERION: Application information is obtained from document registration forms submitted for .bqy scheduling and publishing or entered directly by application content publishers during publishing and scheduling. The application captures usage data when a user logs into the system or retrieves a document. eAuthentication internal id and user name are provided by RD and FSA Information Security staffs or during user self-registration.</p> <p>TDW: Various OLTP systems, including Guaranteed Loan System (GLS), Direct Loan Origination System</p>

FOR OFFICIAL USE ONLY

	<p>(DLOS), Multi-Family Management (MFM), Water and Environmental Programs (WEP), Guaranteed Underwriting System (GUS), Rural Utility Loan Servicing System (RULSS); human resource data from NFC; and data from FSA, Natural Resources Conservation Service (NRCS), and RD for civil rights reporting purposes.</p>
<p>(a). Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?</p>	<p>Electrofiche: The information is taken from loan servicing information entered into the enterprise systems used as report sources.</p> <p>FOCUS/WebFOCUS: Data is retrieved from existing agency files and data bases</p> <p>HYPERION: The system queries data stored in the following databases and passes the information to the requesting client/user. RD: Rural Development Data Warehouse, RULSS Borrower Database Mgmt System (BDMS) and CASH, GLS AASM, GLS KCCDSN, ECMM, and Broadband data. FSA & RD: Program Funds Control System (PFCS)</p> <p>TDW: No information in the TDW comes from individuals. All information in the TDW comes from various OLTP systems as described in question 2 above.</p>
<p>(b). What Federal Agencies are providing data for use in the system?</p>	<p>FOCUS/WebFOCUS: RD, FSA and EPA (a list of waste sites is downloaded from the EPA website).</p> <p>Electrofiche: RD and FSA.</p> <p>HYPERION: RD and FSA provide user information and user to group associations. System Support Division report developers provide .bqy files (pre-defined queries) for the system to execute.</p> <p>TDW: The vast majority of the data is from RD. FSA, NFC and NRCS provide data once every year related to civil rights reporting.</p>
<p>(c). What State and Local Agencies are providing data for use in the system?</p>	<p>None</p>
<p>(d). From what other third party sources will data be collected?</p>	<p>TDW: USDA National Finance Center (NFC) for Human Resource data.</p>
<p>(e). What information will be collected from the customer/employee?</p>	<p>FOCUS/WebFOCUS: Employee login userID and password are provided for logging into the system.</p> <p>Electrofiche: Loan servicing information entered into the enterprise systems used as report sources.</p> <p>HYPERION: User eAuthentication internal id's are</p>

FOR OFFICIAL USE ONLY

	<p>provided for authorizing access to content when the user logs into the system before .bqy, predefined queries are made available for access and processing.</p> <p>TDW: User ids/passwords for employees are established by Security. Other than that, all data is coming from the various OLTP systems, not directly from the employee/customer.</p>
<p>3. Accuracy, Timeliness, and Reliability</p>	
<p>3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?</p>	<p>FOCUS/WebFOCUS: N/A – Data is provided from Rural Development records.</p> <p>Hyperion: Only Rural Development and Farm Services Agency data, customer provided data, and supporting application metadata is supported within the application. Proprietary application metadata supports application functionality and verified during functional application testing.</p>
<p>3b. How will data be checked for completeness?</p>	<p>FOCUS/WebFOCUS: Correct processing and loading of data into reporting systems will be checked by the Operations Scheduling Branch.</p> <p>Hyperion: Content publishers verify that the pre-defined queries return complete results during test and certification activities. Proprietary application metadata is verified as complete during functional application testing.</p> <p>Electrofiche: Data completeness and correctness will be verified by the enterprise source systems. Correct loading of the reports into the system will be checked by the Operations Scheduling Branch.</p> <p>TDW: Validation queries are run to compare data loaded into the data warehouse tables to data content within the input flat files.</p>
<p>3c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).</p>	<p>Electrofiche: Reports are downloaded to the Electrofiche server on a nightly basis.</p> <p>FOCUS/WebFOCUS: Yes, data is refreshed following updates to system databases and files as documented in Subsystem PD Operating Instructions.</p> <p>Hyperion: Content publishers verify that the pre-defined queries will return current results during test and certification activities. Content publishers validate that the queries are scheduled to run and update published documents with current data as it becomes available from the data source. Standard UMAT procedures are used to verify that the application's</p>



FOR OFFICIAL USE ONLY

	<p>metadata contains current user authorization data.</p> <p>TDW: The TDW is reloaded/refreshed nightly with COB data from the various OLTP systems. Automated load processes for the TDW run each night. Any problems with the load processes are systematically detected and reported. Validation queries are run to compare data loaded into the data warehouse tables to data content within the input flat files provided from the various OLTP systems.</p>
<p>3d. Are the data elements described in detail and documented? If yes, what is the name of the document?</p>	<p>Electrofiche: The data is stored in a report format. The field names and values are clearly labeled.</p> <p>FOCUS/WebFOCUS: Yes, data elements are documented in files for mainframe online access and in the Rural Development & Farm Service Agency FOCUS Ad Hoc Reporting System Manuals.</p> <p>Hyperion: Data source owners define data elements for their respective database. Hyperion application metadata data elements are proprietary and is maintained by the software vendor.</p> <p>TDW: The TDW contains two database tables for metadata. The rd_table_metadata includes table name, table description and update frequency. The rd_column_metadata includes table name, column name, description, source and transformation rules if any.</p>

D. ATTRIBUTES OF THE DATA

<p>1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?</p>	<p>FOCUS/WebFOCUS, Electrofiche, TDW: Yes. The data supports application functionality.</p> <p>HYPERION: Yes. The data supports application functionality and .bqy file access.</p>
<p>2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?</p>	<p>FOCUS/WebFOCUS, Electrofiche: No</p> <p>Hyperion: Yes. The system will derive usage statistics identifying the user's application login activity and the documents retrieved from the application by the user.</p> <p>TDW: Data is not created by the TDW. Data is provided from the various OLTP systems and loaded into the TDW. Data aggregations are done in the TDW for historical trending purposes, not for creating previously unavailable data about an individual.</p>
<p>3. Will the new data be placed in the</p>	<p>FOCUS/WebFOCUS, Electrofiche, TDW: N/A</p>

FOR OFFICIAL USE ONLY

individual's record (customer or employee)?	Hyperion: No
4. Can the system make determinations about customers or employees that would not be possible without the new data?	FOCUS/WebFOCUS, Electrofiche, TDW: N/A Hyperion: No
5. How will the new data be verified for relevance and accuracy?	FOCUS/WebFOCUS, Electrofiche, TDW: N/A Hyperion: N/A. Collection of usage statistics is part of the COTS functionality.
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	FOCUS/WebFOCUS: Yes, ACF2 rules restrict access and FOCUS database authority restrictions applied as required. Electrofiche, TDW: N/A Hyperion: Access is limited to application and system administrators using id and password combinations.
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	N/A
8. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	FOCUS/WebFOCUS: Users log on using their userID and password combination, using canned menu options reports are generated. Data can be retrieved by any field in the data source. Electrofiche: Data is retrieved by requesting the retrieval of a report image. Once retrieved, a report can be searched for specific data items, including personal identifiers. HYPERION, TDW: Using secure clients and personal operating system id and password combinations, application developers query data using ODBC connections to the database.
9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?	Electrofiche: The Electrofiche system is an electronic storage system which holds over 1600 types of reports; tax records, loan documents, accounting reports, etc. The reports are used by everyone from accountants who are trying to balance the government checkbook to customer service representatives who are talking to people about their loans. These employees have access to the Electrofiche system. Electrofiche does not create reports. It is an archival/retrieval system to view reports created by other systems. FOCUS/WebFOCUS: Detail and summary reports are used to service loans and grants, and provide

FOR OFFICIAL USE ONLY

	<p>statistical data for agency reporting. Access is restricted to USDA employees.</p> <p>Hyperion: The COTS server gathers usage statistics that identify user system login and document retrieval. This data will be used to monitor system use and is accessible to application and system administrators.</p> <p>TDW: N/A, reports from TDW data are created using Hyperion.</p>
<p>10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)</p>	<p>Electrofiche: Not applicable. Electrofiche does not collect information from individuals. Reports generated from the various OLTP systems that have collected the provided information are fed to Electrofiche.</p> <p>FOCUS/WebFOCUS: None – Data on borrowers extracted from existing RD and FSA records is for RD and FSA use. Capture of usage statistics is utilized in system planning and monitoring.</p> <p>Hyperion: None - Capture of usage statistics is required for system planning and monitoring.</p> <p>TDW: Not applicable. TDW does not collect information from individuals. Data is fed to the TDW from various OLTP systems that have collected the provided information.</p>

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

<p>1. If the system is operated in more than one site, how will consistent use of the system and data will be maintained in all sites?</p>	<p>FOCUS/WebFOCUS: The system is only hosted at one site, NITC.</p> <p>Electrofiche: The data is downloaded from the NITC mainframe and St. Louis web farm servers to one server by OSB schedulers on a scheduled basis.</p> <p>HYPERION, TDW: The system is only hosted at one site, the St. Louis Web Farm.</p>
<p>2. What are the retention periods of data in this system?</p>	<p>FOCUS/WebFOCUS: User access information is retained as long as it is required to provide users access to the system. Application files are maintained until they are replaced or removed by the file creator.</p> <p>Electrofiche: Data is retained for the life of the loan as a minimum.</p> <p>HYPERION: User access information is retained as</p>

FOR OFFICIAL USE ONLY

	<p>long as it is required to provide users access to the system. Applications (.bqy files) are maintained until they are replaced or removed by the publisher.</p> <p>TDW: The last three years of monthly snapshots, and end of calendar year and end of fiscal year snapshots for the fourth and fifth years are retained.</p>
<p>3. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?</p>	<p>FOCUS/WebFOCUS: Users are removed as directed by FSA and RD Information System staffs. The procedure for removing a user is documented in St. Louis.</p> <p>Electrofiche: Current procedures call for the data to be retained for the life of a normal real estate loan, 30 years or more. There is no plan to delete the data.</p> <p>HYPERION: Users are removed RD ISS as directed by requests to FSA and RD Information System staffs. The procedure for removing a user is documented. BQY files are removed from the server by application administrators using document registration forms or by authorized content publishers as defined in program area CM procedures. The procedure for removing a .bqy file is documented.</p> <p>TDW: Although the above guideline has been established for data retention, no historical data is deleted until approval is given by the respective business/program owners/managers. Automated scripts, which contain documentation, have been developed which can be invoked by the TDW database administrator to delete old historical data.</p>
<p>4. Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?</p>	<p>No</p>
<p>5. How does the use of this technology affect public/employee privacy?</p>	<p>FOCUS/WebFOCUS, HYPERION, TDW: N/A</p> <p>Electrofiche: Since Electrofiche is a report delivery system but not a report generating system, its effects are those of the source systems.</p>
<p>6. Will this system provide the capability to identify, locate, and monitor <u>individuals</u>? If yes, explain.</p>	<p>FOCUS/WebFOCUS, HYPERION: Yes. FOCUS & Hyperion are reporting tools and if databases that they report against contain data about an individual that information can be retrieved.</p> <p>Electrofiche: Only insofar as the source system for a report will permit.</p> <p>TDW: Since monthly snapshots of loan making and</p>

FOR OFFICIAL USE ONLY

	<p>loan servicing activities are kept as historical data, related data, such as loan delinquency status over time for instance, for individuals can be retrieved via Hyperion. There is no monitoring capability or processes that are directly spawned by the TDW.</p>
<p>7. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>Electrofiche: Loan servicing information. FOCUS/WebFOCUS: User Id login and logout dates and times. Hyperion: The Hyperion COTS application server collects content usage information including when a user logs onto the application server, what documents are retrieved and the time a document is retrieved. TDW: Loan making and loan servicing actions.</p>
<p>8. What controls will be used to prevent unauthorized monitoring?</p>	<p>FOCUS/WebFOCUS, Electrofiche, HYPERION: Access to the logs is limited to the system and application administrators. TDW: Non-restricted data that can be used for monitoring purposes, as described in question 5.9 above, is accessible via Hyperion to all authorized RD users who have requested Hyperion access and been approved through the RD Security office. No users, other than those approved by Security, can access the data.</p>
<p>9. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.</p>	<p>USDA/RURAL DEVELOPMENT-1</p>
<p>10. If the system is being modified, will the SOR require amendment or revision? Explain.</p>	<p>Rural Development's Systems Development Life Cycle and Configuration Management processes require the ISSS to review system changes for security documentation updates and re-accreditation decisions impact to ensure that the System of Record Notices are revised as needed.</p>

F. ACCESS TO THE DATA

<p>1. Who will have access to the data in the system (E.g., contractors, users, managers, system administrators, developers, tribes, other)?</p>	<p>FOCUS/WebFOCUS, Electrofiche, HYPERION: System administrators, application administrators, developers, and end-users have access to the system. TDW: The database administrator, data warehouse developers, report developers, program managers, and end-users have access to the system.</p>
--	---



FOR OFFICIAL USE ONLY

<p>2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?</p>	<p>Electrofiche: The System Authorization Access Requests (SAAR) request-approving official is responsible for granting each user access to the Electrofiche system.</p> <p>FOCUS/WebFOCUS, HYPERION: Access is controlled by userID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor. The User Access Management Team (UAMT) follow their procedures to provide access to the system. The ISSS personnel approve and process elevated access requests. The procedures are documented.</p> <p>TDW: Access is controlled by user ID and password. Access rights are granted to designated individuals, as requested by RD Security. Security is responsible for maintaining whatever procedures and documents they deem necessary for access control.</p>
<p>3. Will users have access to all data on the system or will the user's access be restricted? Explain.</p>	<p>FOCUS/WebFOCUS: Access is restricted to a need to know basis, by state, county, district, servicing office or loan program.</p> <p>Electrofiche: Currently all users have access to all data on the system.</p> <p>HYPERION: Users do not have access to all data. Access to .bqy files (predefined queries) is governed by group membership. BQY files are published for access by specified groups. If a user is not in a group that has access to a .bqy file, it will not be presented for the user.</p> <p>TDW: Most of the data within the TDW is accessible to all authorized RD users who have requested access through their supervisor and processed by the ISSS office; however, the human resources data, PFCS data, and RULSS bank account information are restricted.</p>
<p>4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?</p>	<p>FOCUS/WebFOCUS: ACF2 rules restrict access and FOCUS database authority restrictions are applied as required.</p> <p>Electrofiche: Standard network security and RD ISSS policy and procedures.</p> <p>HYPERION: Access to the data is restricted to the</p>



FOR OFFICIAL USE ONLY

	<p>application administrator and developers at the table level based on required functionality. Browsing of system directories is restricted by the web server configuration.</p> <p>TDW: The Human Resources data is restricted at the database level. All other restricted data is restricted at the respective table level.</p>
<p>5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, are Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?</p>	<p>Electrofiche: Yes, contractors are involved and the contracts contain Privacy Act contract clauses.</p> <p>FOCUS/WebFOCUS: St. Louis ISSS contractors maintain mainframe FOCUS database authority by User Id only. Privacy Act clauses are in the ISSS contracts.</p> <p>Hyperion: Yes, contractors are used in design and development activities. Yes, the contract includes Privacy Act contract clauses and addresses other regulatory matters.</p> <p>TDW: Yes, contract contains Privacy Act clause.</p>
<p>6. Do other systems share data or have access to data in this system? If yes, explain.</p>	<p>FOCUS/WebFOCUS: Yes, interface with the GLS: Guaranteed Loan System DB2 reporting tables and with specific IDMS databases (MSTR: Multi-Family Housing application data, & CTRK: Cash Tracking data). RD / FSA data is extracted from databases and files (DLOS: Direct Loan Origination and Servicing, & PLAS: Program Loan Accounting System).</p> <p>Electrofiche: Reports loaded into the Electrofiche system come from other OLTP systems.</p> <p>TDW: Data from the OLTP systems is provided in flat files for loading into the various data marts. Data can be retrieved from the TDW by Brio queries, which can then be used in OLTP systems as needed.</p> <p>HYPERION: Yes. The Hyperion connects thru a ODBC connection to several different data sources. Hyperion then queries these sources from developed stored procedures and displays the results to the user or exports them to a predetermined media. Hyperion itself has no data to share.</p>
<p>7. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface?</p>	<p>Automated Mail Processing (Janet.Havelka@stl.usda.gov), Commercial (Brenda.Operle@stl.usda.gov), Consumer (Janet.Havelka@stl.usda.gov), eGovernment Services (Kathy.Anderson@stl.usda.gov), Enterprise Content Management (Edward.Koenen@stl.usda.gov), Guaranteed (Greg.Eschman@stl.usda.gov), Imaging (Kathy.Anderson@stl.usda.gov), Multi-Family</p>



FOR OFFICIAL USE ONLY

	<p>Management (Glennon.Boeckmann@stl.usda.gov), Program Funds Control System (Janet.Havelka@stl.usda.gov). Rural Utilities Service – Legacy (Enrique.Perez@wdc.usda.gov)</p>
<p>8. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?</p>	<p>FOCUS/WebFOCUS: No. The system use is limited to Rural Development and Farm Services Agency and Office of the Inspector General authorized personnel. Electrofiche, HYPERION: No. The system use is limited to Rural Development and Farm Services Agency authorized personnel. TDW: Other than RD, data is furnished by NRCS, FSA, and NFC (RD human resource data only).</p>
<p>9. How will the data be used by the agency?</p>	<p>Electrofiche, Hyperion, FOCUS/WebFOCUS: Reporting purposes. TDW: The data is used to produce mission-critical reports and provide business intelligence, which facilitates sound management decisions that efficiently and effectively support the needs of Rural Development customers.</p>
<p>10. Who is responsible for assuring proper use of the data?</p>	<p>Automated Mail Processing (Janet.Havelka@stl.usda.gov), Commercial (Brenda.Operle@stl.usda.gov), Consumer (Janet.Havelka@stl.usda.gov), eGovernment Services (Kathy.Anderson@stl.usda.gov), Enterprise Content Management (Edward.Koenen@stl.usda.gov), Guaranteed (Greg.Eschman@stl.usda.gov), Imaging (Kathy.Anderson@stl.usda.gov), Multi-Family Management (Glennon.Boeckmann@stl.usda.gov), Program Funds Control System (Janet.Havelka@stl.usda.gov), Rural Utilities Service – Legacy (Enrique.Perez@wdc.usda.gov)</p>



FOR OFFICIAL USE ONLY

APPENDIX A

DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the USDA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

FOR OFFICIAL USE ONLY

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

FOR OFFICIAL USE ONLY

APPENDIX B

POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility, which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.