UNITED STATES DEPARTMENT OF AGRICULTURE

FARM SERVICE AGENCY

Privacy Impact Analysis (PIA)
for
Consolidated Administrative Systems – WDC
(CAS-WDC)

- WDC Web Based Administrative Systems
- WDC Focus Administrative Systems
- WDC Client/Server Administrative Systems
- WDC Former IPUSO Applications

FINAL

Update Date: August 27, 2007

Accreditation Date:

Farm Service Agency
FSA/DAM/ITSD/GIEMSC/EMSO
1400 Independence Avenue, SW
Washington, DC 20250

Document Control

Date	Source	Author	Description of Changes
02/23/2007	Template	J Wagner, EDS	Original document.
02/23/2007	2006 Client Server PIA	J Wagner, EDS	Copied in PIA from 2006
02/23/2007	2006 Focus PIA	J Wagner, EDS	Copied in PIA from 2006
02/23/2007	2006 Web-based PIA	J Wagner, EDS	Copied in PIA from 2006
03/12/2007	O Torres, EMSO	O Torres, EMSO	Remove obsolete PIAs, correct typo for GIEMSC in system descriptions.
3/15/2007	D Stukes, EMSO	D Stukes, EMSO	Complete entries for Web eRTS
3/15/2007	O Torres, EMSO	O Torres, EMSO	Complete entries for Web EOTS Reporting
3/21/2007	J Cuffee EMSO	J Cuffee EMSO	Completed eWIMS & All but 5a for CRS
3/22/2007	D Stukes, EMSO	D Stukes, EMSO	Complete entries for Accessions systems
3/22/2007	D Stukes, EMSO	D Stukes, EMSO	Complete entries for Youth USDA Mentoring and Tutoring Program
3/22/2007	D Stukes, EMSO	D Stukes, EMSO	Complete entries for Non-PO Tracking System
3/22/2007	D Stukes, EMSO	D Stukes, EMSO	Complete entries for SF-39 Metrics System
3/23/2007	G Joseph EMSO	G Joseph EMSO	Updated entries for IPIA
3/26/2007	G Joseph EMSO	G Joseph EMSO	Updated entries for PTS
3/26/2007	G Joseph EMSO	G Joseph EMSO	Updated entries for WIS
3/26/2007	G Joseph EMSO	G Joseph EMSO	Updated entries for RFA
3/28/2007	D Stukes EMSO	D Stukes EMSO	Updated entries for SF-52
3/28/2007	J Cuffee EMSO	J Cuffee EMSO	Completed CRS & TAL

3/29/2007	O Torres, EMSO	O Torres, EMSO	Update Section 2.2.1 System Applicability table, move YUMTP, RFA, PTS applications from Web subsystem into Former IPUSO subsystem tables and removed obsolete IPUSO applications from table. Update section 2.2.4 Former IPUSO system overview description. Modify section 3.1 move YUMTP, SF52 responses from Web subsystem to section 3.4 Former IPUSO. Modify system overviews to match FSA inventory line up of systems.
04/04/2007	O Torres, EMSO	O Torres, EMSO	Correct CORP and move and rename as SCORP under Web
04/05/2007	O Torres, EMSO	O Torres, EMSO	Updates to IMS,Flotrack,TMS,Web52,Warmis,SCORP
04/25/2007	O Torres, EMSO	O Torres, EMSO	Remove “Sybase” from Client/Server Subsystem Name in System Applicability Table
	F Wesolowski, EMSO	F Wesolowski, EMSO	System Owner Approve
	J Wagner, EDS	J Wagner, EDS	C&A SME approve
04/06/2007		Eric Miller, ISO	C&A Phase 1 ISO approved
08/07/2007	OCIO Template	J Wagner, EDS	Added Signature Page
08/15/2007		Brian Davies, ISO	Made spelling and syntax corrections
08/27/2007	FSA	J Wagner, EDS	Marked as final

Prepared for:
Certification & Accreditation
Farm Service Agency
United States Department of Agriculture
6501 Beacon Dr.
Kansas City, MO 64133

Table of Contents

Table of Tables

1 Purpose of Document

USDA DM 3515-002 states: “Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in USDA.

Both the system owners and system developers must work together to complete the PIA. System owners must address what data are used, how the data are used, and who will use the data. System owners also need to address the privacy implications that result from the use of new technologies (e.g., caller identification). The system developers must address whether the implementation of the owner’s requirements presents any threats to privacy.”

The Privacy Impact Assessment (PIA) document contains information on how the Consolidated Administrative Systems - Washington, DC affects the privacy of its users and the information stored within. This assessment is in accordance with NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems.*

2 Applicability

2.1 Applicability of System

The information in this document is applicable to the system and its subsystems as listed below.

Table 1: System Applicability

System	Subsystem
Consolidated Administrative Systems – Washington, DC (CAS-WDC)	• **WDC Web Based Administrative Systems** o Contact Search Employee Directory o eCalendar o External Oversight Tracking System o Farm Loan Officer Tracking System (FLOTrack) o Operations, Review, and Analysis System o State Directive Management o Telework Management System (TMS) o Web 52 Phase I and 2 o Inventory Management System (IMS) o Sweetener Market Data Application o Electronic Foreign Service Retirement System (eFSRS) o Electronic Warehouse Inventory Management System (eWIMS) o Electronic Regulation Tracking System (eRTS) o Improper Payments Information Act (IPIA) o State & County Operations Review Program (SCORP) • **WDC Former IPUSO apps** o Accessions o SF-39 Metrics System-Personnel Exam Activity Tracking System o Non-PO Tracking System o SF-52 Personnel Action System o Warehouse Inventory System o Travel Allocation Log o ASD Key Tracking Process o Youth USDA Mentoring and Tutoring Program o The Procurement Tracking System (PTS) o The Request for Action (RFA) • **WDC Focus Administrative Systems** o Executive Information System (EIS) o Warehouse Rates Management Information Sys, WDC (Replacing with web-based Q4/07) o Compliance Reporting System (CRS) • **WDC Client/Server Administrative Systems** o Warehouse Inventory Management System (WIMS) (Replacing with web-based Q4/07) o Regulation Tracking System External Oversight Tracking System (EOTS)

2.2 System Overview

EMSO builds applications to facilitate managers and employees supporting the agency mission. Our applications usually gather or report information, or track the progress of tasks. Many applications have a database to collect or provide the information tracked. The front end was formerly windows clients (or stand alone applications) but most applications are now developed or converted to web based applications. Almost all applications are only accessible from within the FSA network (inside agency firewalls). There are many legacy applications which were developed in focus, or client/server, or even desktop applications.

2.2.1 WDC Web Based Administrative Systems

Most of the newer applications and applications that are being enhanced are web based. The web based applications include: Contact Search Employee Directory, eCalendar, EOTS Reporting, FLOTrack, ORAS, SDMS, TMS, Web52, IMS, SMDA, eFSRS, eWIMS, eRTS, IPIA and SCORP. All applications are developed by FSA/DAM/ITSD/GIEMSC/EMSO. All use IIS as the web server and most use SQL-Server as the database. The web and database servers will be at the NITC facility by the end of fiscal ’07. Most applications are eAuthentication enabled and only accessible from within the FSA network.

2.2.2 WDC Focus Administrative Systems

The Focus legacy applications include: EIS, WARMIS, and CRS. EIS is a client/server application that resides on the Microsoft Active Directory Network and WARMIS reside on the DEC mini computer. All applications are developed by FSA/DAM/ITSD/GIEMSC/EMSO. EIS, CRS and WARMIS use Focus v6 as its database management tool. The programming languages include Focus v6, COBOL, and SQL. WARMIS will be retired by the end of fiscal ’07. All are only accessible from workstations within the agency firewall and have no external connectivity.

2.2.3 WDC Client/Server Administrative Systems

The Client-Server legacy systems include: WIMS, RTS and EOTS. All applications were developed in-house by FSA/DAM/ITSD/GIEMSC/EMSO. The front end was usually developed in Visual Basic and the backend is (or will be by the end of fiscal ’07) SQL-server. All are only accessible from workstations within the agency firewall and have no external connectivity.

2.2.4 WDC Former IPUSO Applications

The legacy applications inherited from the IPUSO office after the realignment of missions include standalone applications, a couple of SAS mainframe applications and a few web based applications. All are only accessible from workstations within the agency firewall and have no external connectivity. Most systems have less than 8 users. These applications include: Accessions, SF-39 Metrics, NPOTS, SF52-PAS, WIS, TAL, ASD-KTP, YUMTP, PTS and RFA.

3 USDA PRIVACY IMPACT ASSESSMENT

[This Page Intentionally Left Blank]

3.1 Web Based Administrative Systems (WBAS)

WBAS Table 2: Data In The System

DATA IN THE SYSTEM	
1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	[eFSRS] Data in system is used in processing retirements of FAS employees. Customer: FSA Human Resource Division (HRD) staff. Customer data: EAuthentication identifier, Name, Shared Employee Id Employee data: Shared Employee Id, SSNO, Birth Date, Is Active Employee, and Name are obtained from a read-only view of Shared. Information on Organization, Pay Plan Series, and Base Pay (for Virtual Locality Pay calculation), Official Station, and Contributions and Actions data are retrieved from NFC system. Data is only retrieved from NFC and is not updated [Web 52] Application is used by FFAS employees in performance of their duties and contains information about FFAS employees. There is no use/access to others. Employee is Customer. Used by FFAS program area managers/administrative assistants to create and track an SF52 form. These users have access to employees in their organization. Once the user selects the employee, the grade/step and salary are displayed. HR users have access to the personnel data of the employee for which the SF-52 is processed. Employee data includes name, social security number, date of birth and an employee's position information (grade/step/salary), as well as comments from supervisors. [eCalendar] FFAS employees are customers. Employees will see event start date, end date, location, and event category and organization name. [SDMS] SDMS Tracks stage of directive in progress of approval. Employees are customers from HQ, State, Division, Branch offices. Employees: first name, last name, phone, email, state, user category, directive ID, directive create date, user proxy, approval status. [EOTS Reporting] Access restricted to security type "Confidential" and Managers only for Customer : Producer Last Name, First Name, State, City, County (Data is collected on Audits, Investigations and Hotline Complaints subsystems) Access restricted to security type "Confidential" and to Managers only for Employee: Employee Last Name, First Name, State, City, County(Data is collect on

DATA IN THE SYSTEM	
	Investigations and Hotline Complaints subsystems) [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] System data is used to manage the administrative flow of regulations from inception to publication in the Code of Federal Regulations. Federal Employees as well as the public have an opportunity to state comments on proposed rules. [IPIA] Employees: USDA employees are users of the application. Only first name, last name is displayed. Customers: Tax ID Numbers (TIN) relating to program payments are displayed. These numbers are encrypted in the database and the application is protected by SSL. [SCORP] Customer: ORAS Other : Information stored in database.(Exhibit Number, Findings, Reported Year, username, handbook number)
2a. What are the sources of the information in the system?	[TMS] Telework requests are entered by employees and additional data is provided by National Finance Center (NFC) downloads. [Flotrack] Original information is manually entered in its entirety by the Field Loan Office (FLO) trainees, their supervisors and management staff, and/or system administrators. [ORAS] Information comes from FSA State and county office program and administrative operations. [Contact Search] System is update National Finance Center (NFC) downloads. FFAS employee provides updates to email room and phone number to keep information current. [SMDA] System is updated with data from Sugar Companies on a monthly basis. [IMS] Supply transactions and orders entered by supply room employees. [eFSRS] NFC downloads , HRD User input [Web 52] NFC, user input. [eCalendar] Meetings and events entered into the system by FFAS employees. [SDMS] Information for State directives is entered by FSA State offices. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question.

DATA IN THE SYSTEM	
	[eRTS] System will initially be updated with old RTS data. Regulatory Review Group, FSA, will maintain and update this system. [IPIA] Information displayed on the system is provided by ORAS (USDA/FSA/OA/OBPI/ORAS) in the form of spreadsheets that were imported into the application. [SCORP] Output from CORP(County operations reviewers program) to SCORP Reporter DB
2b. What USDA files and databases are used? What is the source agency?	[TMS] Shared DB. FSA [Flotrack] The FLOTrack system database is entirely self-contained. FSA [ORAS] ORAS DB, FSA [Contact Search] ContactSearch DB [SMDA] SMDA DB, FSA [IMS] IMS, Shared DB FSA [eFSRS] Fsrs, Shared DB FSA [Web 52] Shared, Web52 DB FSA [eCalendar] eCalendar DB [SDMS] SDMS DB [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] RTS DB FSA [IPIA] IPIA uses its own database and displays information provided by ORAS. [SCORP] SCORP Reporter DB, ORAS (Operations Review and Analysis Staff)
2c. What Federal Agencies are providing data for use in the system?	[TMS] National Finance Center (NFC) - FFAS. Data is downloaded from NFC to Shared. Data is retrieved from Shared by using customized views. [Flotrack] None [ORAS] None [Contact Search] NFC -FFAS [SMDA] - None [IMS] NFC – FSA. Data is downloaded from NFC to Shared. We retrieve data needed from Shared by using customized views. [eFSRS] NFC-FAS [Web 52] FFAS [eCalendar] None [SDMS] National Finance Center (NFC) - FFAS. Data is downloaded from NFC to Shared. Data is retrieved

DATA IN THE SYSTEM	
	from Shared by using customized views. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [IPIA] N/A [SCORP] N/A
2d. What State and Local Agencies are providing data for use in the system?	[TMS] FFAS (DC and KC) [Flotrack] State offices (via end-user input as stated above). [ORAS] All FSA state and county offices. [Contact Search] FFAS (DC and KC) [SMDA] None [IMS] None [eFSRS] None [Web 52] None [eCalendar] None [SDMS] None [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] FSA Offices and the Office of the Federal Register [IPIA] N/A [SCORP] State and County Office USDA Offices
2e. From what other third party sources will data be collected?	[TMS] None [Flotrack] None [ORAS] None [Contact Search] None [SMDA] Sugar Companies [IMS] None [eFSRS] None [Web 52] None [eCalendar] None [SDMS] None [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Public comment.

DATA IN THE SYSTEM	
	[IPIA] County Operations Reviewers who work under ORAS will complete questionnaires and provide details on over or under payments. [SCORP] State and County Office USDA Offices
2f. What information will be collected from the customer/employee?	[TMS] Phone #, Email address, User Interface preferences, and telework residences. [Flotrack] User email account, managers name, state office, telephone number, job title, machine-generated sequential id, date hired, office location, training modules completed, test answers, test completion dates, test scores; self comments, management comments, overall requirements met (or failed to be met), final status (including qualified, resigned, active, terminated, deceased.) [ORAS] Customers County Office Review (COR) Actions, Holidays, Staff COR Time are collected. [Contact Search] Phone #, Email address, User Interface preferences [SMDA] Sugar supplied and distributed from all the domestic sugar beet processors, sugar cane processors and cane refiners. [IMS] Supply orders and transactions – only used by supply room staff [eFSRS] Primary purpose of application is not data collection. The only input employee data by HRD is Service Credit Payments based upon physical checks received by HRD. [Web 52] Program area users input comments justifying requested personnel actions, HR users input personnel actions. [eCalendar] Event start date, end date, event time location, Employee name. [SDMS] State office employees create and submit directives for approval or clearance by the National Office. They also track directives within their own state and view directive status. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] The Regulatory Review Group will solicit comment and approval of a proposed new rule or law. [IPIA] No employee information is collected. The only information collected is the completion of the questionnaires to determine the reasons for over or under payments.

DATA IN THE SYSTEM	
	[SCORP] Issues and Problems that are discovered by the county operations reviewers (COR)
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	[TMS] None [Flotrack] None collected outside of the USDA. [Contact Search, ORAS, eFSRS] None [SMDA] Business rules and validations. [IMS] None [Web 52 None collected outside of the USDA. [eCalendar] None [SDMS] None [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] None [IPIA] N/A [SCORP] Business rules and validations.
3b. How will data be checked for completeness?	[TMS] Required field, and regular expression validations, business rules. [Flotrack] No non-USDA data is collected. All fields are input by USDA personnel. Required field and regular expression validations. [ORAS] Required field and regular expression validations. [Contact Search] Client side field validations. [SMDA] Required field and regular expression validations. [IMS] Input restrictions and field validation. [eFSRS] HRD checks for accuracy. NFC downloads provide updates. Corrections are incorporated via a biweekly feed. [Web 52] Some validation is built in the application, and some are provided by HR processes. [eCalendar] Input restrictions and field validation. [SDMS] Input restrictions and field validation. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Input restrictions and field validation. [IPIA] N/A [SCORP] Required field validation, regular expression validations.

WBAS Table 3: Access To The Data

ACCESS TO THE DATA	
1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	[TMS] Users have access by using role-based views (User Interface views). All data and operations are protected by role-based in-depth permission validation. Application account and DB account have restricted access to the application DB. DB administrator (DB objects) has full access. [Flotrack] FLO Trainees can review their own information, comments, preferences, personal profile information. Can take tests on line and view requirements met; FLO Managers can review information concerning the trainees who report to them; FLO Coordinators/Chiefs can review for all trainees in their states or areas of responsibility. Can also register new users to a pending status; National office users can review all information for all trainees in all states; National system administrator can view all data, activate new users registered by FLO chiefs/coordinators, archive user records, and make corrections to and/or limited deletions of erroneous data. [ORAS] ORAS administrators, managers and field officers. [Contact Search] All FFAS Users have view only access for searching employee specific data. Data operations have been protected by validations using last four digits of social security number with last name and date of birth. Application account and DB account have restricted access to the application DB. [SMDA] Users have access by using role-based views (User Interface views). All data and operations are protected by role-based in-depth permission validation. Application account and DB account have restricted access to the application DB. DB administrator (DB objects) has full access [IMS]: Supply room users. Application and Database Account have restricted access to database. DB administrator has full access. [eFSRS] HRD Users [Web 52] Application is used by FFAS employees in performance of their duties and contains information

ACCESS TO THE DATA	
	about FFAS employees. There is no use/access to customers or others. Used by FFAS program area managers/administrative assistants to create and track an SF52 form. These users have access to a list of names of employees in their organization. Once the user selects the employee, the grade/step and salary are displayed. Used by HR to process and track an SF52 form. HR users have access to the personnel data of the employee for which the SF-52 is processed. This data includes name, social security number, date of birth and an employee's position information (grade/step/salary), as well as comments from supervisors. [eCalendar] FFAS Users [SDMS] State User, national user, administrators based roles [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Regulatory Review Group. [IPIA] Admin: ORAS National Office employees Reviewer: ORAS County Operations Reviewers [SCORP] Users by using role-based views (UI views). All data and operations are protected by role-based in-depth permission validation.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	[TMS] eAuthentication and Role-based security check. [Flotrack] Data access is role based and only authenticated FLOTrack users are allowed access. New users are entered by National System administrator and Flo Chief/Coordinators only. [ORAS] Access to data is determined by roles built into the application. [Contact Search] If data is modified by the user then validations are done using the last four digits of social security number with last name and data of birth. [SMDA] Role-based security check. [IMS]: eAuthentication [eFSRS] Application will be protected by eAuthentication. [Web 52] During the design process, type of access Program Area (PA), Human Resource (HR) for access to information was determined by HR based on applicable laws and regulations. The type of access is

ACCESS TO THE DATA	
	documented in the requirements document. [eCalendar] No access restrictions. Any USDA user with access to a browser can access application. However only events that are valid and that originate from FFAS users are approved. [SDMS] Access to data is determined by roles built into the application. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Access to data is determined by roles built into the application. [IPIA] Users need to use their eAuth accounts to log into the application, but only a limited number of ORAS employees can log in. New users are added only through direct request by the ORAS National Office project sponsors. Application logic restricts some functions to users with an Admin role only. [SCORP] Role-based security check.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	[TMS] Access to data is restricted based on user permission set (roles). Release 1.0 – Applicant, Supervisor, Human Resource Division (HRD approver), Telework Monitor roles. Applicant and HRD Approver roles can see home address and last 4 digits of applicant's SSN. Supervisor and Telework Monitor are able to see last 4 digits of applicant's SSN. [Flotrack] Access is restricted based on user role, which is granted within FLOTrack by National System administrator and/or State-level Flo Chief/Coordinator. [ORAS] Access to data is restricted. Users will see data only relevant to their roles. [Contact Search] All FFAS users will have access to view only data. [SMDA] Access to data is restricted. Based on user permission sets (roles). [IMS]: No roles. All authorized users can access all parts of the application. [eFSRS] Application is used only by a very limited number of HRD users. There are no roles and all application information is accessible by all users. [Web 52] Application is used by FFAS employees in performance of their duties and contains information about FFAS employees. There is no use/access to customers or others.

ACCESS TO THE DATA	
	Used by FFAS program area managers/administrative assistants to create and track an SF52 form. These users have access to a list of names of employees in their organization. Once the user selects the employee, the grade/step and salary are displayed. Used by HR to process and track an SF52 form. HR users have access to the personnel data of the employee for which the SF-52 is processed. This data includes name, social security number, date of birth and an employee's position information (grade/step/salary), as well as comments from supervisors. [eCalendar] Any FFAS user can input conference room requests. However, a manager or an administrator will review the requests and approve/reject requests based on availability and legitimacy of requests. [SDMS] Access to data is restricted and is based on user permission set roles. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Access to data is restricted and is based on user permission set roles. [IPIA] Roles are managed in the application database. [SCORP] Access to ORAS Specialists only.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	[TMS] Role-based security check; Release 1.0 – partial display of SSN. [Flotrack] Role-based security checking; all data access controlled via stored procedures which using MS SQL Server security to authenticated users. [ORAS] Application logic built to take care of this scenario. [Contact Search] Application is hosted on the FFAS intranet. [SMDA] Role-based security check [IMS]: eAuthentication protected intranet application. Data is only input into IMS database and does not touch other systems. No sensitive data is accessed or input. Auditing features track activity in specific areas of the application. [eFSRS] Application has auditing features that record users who performed specific functions. Misuse risk is low since application is used only by a very limited number of HRD users.

ACCESS TO THE DATA	
	[Web 52] Application access is controlled by eAuthentication. [eCalendar] Manager approval is required to process conference room requests. [SDMS] Role-based security check. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Role-based security check [IPIA] EAuthentication and role management is used to prevent authorized users from accessing features that are not available to them. Users in the Admin role can add or remove County access permissions for reviewers. [SCORP] Role-based security check
5a. Do other systems share data or have access to data in this system? If yes, explain.	[TMS] No [Flotrack] No [ORAS] No [Contact Search] No [SMDA] No [IMS] No [eFSRS] No [Web 52] No [eCalendar] No [SDMS] No [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] RTS currently has data, until conversion is complete. [IPIA] There is not direct access to this system. However, users in the Admin role can export data, which is ultimately consumed by a SAS application. The details are outside the scope of the project. [SCORP] No
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	[TMS] N/A [Flotrack] N/A [ORAS] N/A [Contact Search] N/A [SMDA] N/A [IMS]: N/A

ACCESS TO THE DATA	
	[eFSRS] N/A [Web 52] N/A [eCalendar] N/A [SDMS] N/A [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Application (security check) and authorized users. [IPIA] No customers access this application. Only limited employee information is displayed. The tax ID number is only viewed by authorized employees of the Farm Service Agency. The data stored in the database is encrypted protecting the information that is stored on the server. [SCORP] N/A
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	[TMS] No [Flotrack] No [ORAS] No [Contact Search] FFAS [SMDA] No [IMS] No [eFSRS] No [Web 52] No [eCalendar] No [SDMS] No [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] No [IPIA, SCORP] No
6b. How will the data be used by the agency?	[TMS] N/A [Flotrack] N/A [ORAS] N/A [Contact Search] Agencies will keep the employees profile up to date. [SMDA] N/A [IMS] Data will be used to track inventory supplies. [eFSRS] N/A [Web 52] N/A [eCalendar] N/A [SDMS] N/A [EOTS Reporting] See response under EOTS

ACCESS TO THE DATA	
	Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA,SCORP] N/A
6c. Who is responsible for assuring proper use of the data?	TMS] N/A [Flotrack] N/A [Contact Search] Contact Search application and authorized users. [ORAS] N/A [SMDA] N/A [IMS] N/A [eFSRS] N/A [Web 52] N/A [eCalendar] N/A [SDMS] N/A [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA,SCORP] N/A

WBAS Table 4: Attributes Of The Data

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. See section 2.2 for usage/mission of each component.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	[TMS] Yes. Dynamically assigned some additional application-specific user attributes based on existing employee's data (supervisory status, e.g.) [Flotrack] Yes. The system will determine whether the FLO trainee has met the requirements to become a Federal Loan Officer. [ORAS] Yes [Contact Search] Employees or Secretaries can update the employees profile to keep their profile current. (supervisory status, Phone number e.g.) [SMDA] Yes, monthly inputs from the sugar companies. [IMS]: No [eFSRS] Virtual locality pay (VLP) is calculated based upon a simple multiplier

ATTRIBUTES OF THE DATA	
	[Web 52] New SF-52 form [eCalendar] No [SDMS] Yes. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] No [IPIA] No [SCORP] Yes, monthly inputs from the State and County Offices.
2b. Will the new data be placed in the individual's record (customer or employee)?	[TMS] No. These data derived automatically and used per-session basis. [Flotrack] Yes. [ORAS] No [Contact Search] Yes. [SMDA] No. These data derived automatically and used per-session basis. [IMS]: N/A [eFSRS] VLP information is indicated in remarks relating to employee actions [Web 52] Form is input to NFC then kept on file at HR [eCalendar] N/A [SDMS] Yes. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA] N/A [SCORP] Yes
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	[TMS] No [Flotrack] Yes, based on pre-defined business rules which define the qualifications for FLOs. [ORAS] No [Contact Search] No [SMDA] No [IMS] N/A [eFSRS] No [Web 52] No [eCalendar] N/A

ATTRIBUTES OF THE DATA	
	[SDMS] No [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA,SCORP] N/A
2d. How will the new data be verified for relevance and accuracy?	[TMS] Business rule verification [Flotrack] Each determination is made based on a distinct set of possible states: (e.g., Test Passed, Test Failed, Test Not Taken) [ORAS] By comparing with other received sources. [Contact Search] Business rule verification [SMDA] Business rule verification [IMS] N/A [eFSRS] HRD has reviewed calculations and business rules being used as well as scripts being used to extract data from NFC. HRD users will manually verify data and can make changes to remarks, as needed. [Web 52] HR user [eCalendar] N/A [SDMS] Business rule verification [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA] N/A [SCORP] Business rule verification
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	[TMS] Role-based controls. [Flotrack] Access to all data, including aggregations is role based as described above. [ORAS] Application built with security for data access. [Contact Search] Validation controls. [SMDA] Role-based controls. [IMS] N/A [eFSRS] N/A [Web 52] N/A [eCalendar] N/A [SDMS] Role-based controls. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question.

ATTRIBUTES OF THE DATA	
	[eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA] N/A [SCORP] Role-based controls.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	[TMS] Role-based controls. [Flotrack] No consolidation. [ORAS] Access is based on log on id, allowing only authorized users to access the system. [Contact Search] Validation controls. [SMDA] Role-based controls. [IMS] N/A [eFSRS] N/A [Web 52] N/A [eCalendar] N/A [SDMS] N/A [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] N/A [IPIA] N/A [SCORP] Role-based controls.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	[TMS] Yes, by personal identifier and set of roles. Mainly, user is identified based on USDA eAuthentication ID. For first time, user is identified based on First/Last name pair and data in Shared DB. If it is not possible to uniquely identify user, TMS asks last four SSN digits or SSN to complete authentication process. eAuthentication ID is stored in TMS DB. Access to all data is verified by TMS based on user attributes and roles. [Flotrack] By User Name, user email address, internal machine-generated user id. [ORAS] Data is retrieved through application screens and reports. Data is accessed by eAuthentication ID and password. [Contact Search] Yes, by personal identifier and set of rules. [SMDA] Yes, by company profile and set of roles. [IMS] User is identified based on USDA

ATTRIBUTES OF THE DATA	
	eAuthentication ID [eFSRS] Foreign service employee data relevant to retirement (contributions and actions) is extracted from the NFC database based upon the officer category (FO, FP, or FE) Data is retrieved by employee name. [Web 52] Data is retrieved by employee name. [eCalendar] Data is retrieved through application screens and event searches. [SDMS] Yes, by personal identifier and set of roles. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Data is retrieved through application screens and event searches. [IPIA] Data records are retrieved using County and Program Codes. This is not sensitive data. [SCORP] Data is retrieved by Role based check, and by the Exhibit chosen.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	No known impacts.
4c. How are the effects to be mitigated?	N/A

WBAS Table 5: Maintenance Of Administrative Controls

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	[TMS, Flotrack, SMDA] All employees within a given role are treated equally by the system, based on pre-defined business rules. [ORAS] Access is permitted for Operations Review & Analysis Staff (ORAS) of FSA. [Contact Search] All employees within a given role are treated equally by the system, based on pre-defined business rules. [IMS] System is 508 compliant and was built specifically for ease of by supply room staff [eFSRS] Application will be Section 508 compliant and

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	will follow USDA style guidelines for look/feel. [Web 52] System provides capability to track personnel actions thus facilitating review. [eCalendar] Any FFAS user can submit meeting room requests. However the manager or administrator will have to approve the request. [SDMS] All employees within a given role are treated equally by the system, based on pre-defined business rules. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] All employees within a given role are treated equally by the system, based on pre-defined business rules [IPIA] Not applicable given the limited scope of the application and the type of data displayed and collected. [SCORP] N/A
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?	[TMS] TMS is operated in one site [Flotrack] While the system will be accessed in multiple locations, all processing and data storage will occur in one site [ORAS] ORAS is a web based system operated from one web-server [Contact Search] Contact search is operated in one site [SMDA] SMDA is operated in one site [IMS] Only operated at one site [eFSRS] N/A [Web 52] One database accessed from multiple sites [eCalendar] Only operated at one site [SDMS] Only operated at one site [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Only operated at one site [IPIA] This is a web-based application, and while the system will be accessed in multiple locations, all processing and data storage will occur in one site only (this is not a distributed application). [SCORP] SCORP Reporter is operated in one site (

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	intranet application on FFAS)
2b. Explain any possibility of disparate treatment of individuals or groups.	[TMS] Individuals are treated the same way. Users may be treated differently than other users only if they assigned different roles (different permissions) [Flotrack] None known. [ORAS] Individual is treated the same way. [Contact Search] Individual is treated the same way. [SMDA] Individual is treated the same way. [IMS] Individuals are treated the same way [eFSRS] Application will be Section 508 compliant. [Web 52] None, users within a role type are treated equally [eCalendar] None known. [SDMS] None known. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] None known. [IPIA] N/A [SCORP] Individual is treated the same way.
2c. What are the retention periods of data in this system?	[TMS] System just released. 3-5 years, at least. [Flotrack] Not Defined. Presumably, the FLO information should be kept in at least an archive status, indefinitely. [ORAS] Data is stored for historical purposes as of now. [Contact Search] System is in production from 3 years. A new and improved system will be replacing the contact search application. [SMDA] System is in production from last 3 years. [IMS] System just released in past year. Large amounts of data are not being captured. 5 years at least. [eFSRS] All historical data is retained. Application only handles a small number of employee's data (~200) and no separate archival needs have currently been identified. [Web 52] Employee data is updated biweekly from NFC, length of retention of SF-52 form is controlled by HR. [eCalendar] All historical data is retained. [SDMS] All historical data is retained.

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	[EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] All historical data is retained. [IPIA] No archival strategy has been identified as of now. The sponsor has indicated that data might potentially be discarded each fiscal year, but a final decision has not been reached on this issue. The relatively low volume of data we are dealing with does not make this a pressing matter. [SCORP] System is in production from last 3 years.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	[TMS] Archiving [Flotrack] Deletion procedures are undefined. Individual records may be flagged as archived or un-archived in real time, at the discretion of the System administrator. [ORAS] N/A [Contact Search] Not defined by business owners. Presumably, archiving. [SMDA] Not defined by business owners. Presumably, archiving. [IMS] Not currently defined by business owners. Presumably, archiving. [eFSRS] Not currently defined by business owners. [Web 52] HR [eCalendar] Not defined by business owners. [SDMS] Not defined by business owners. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Not defined by business owners. [IPIA] N/A Even if data were to be discarded, ORAS will have already consumed the same data in the SAS application. [SCORP] Not defined. Presumably, archiving.
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?	[TMS] NFC downloads occur on biweekly basis. NFC data is compared to application data, and application data is updated to reflect changes from NFC for supervisory status or agency. [Flotrack] Not defined. [ORAS] N/A

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	[Contact Search] Not defined. [SMDA] Not defined. [IMS] N/A [eFSRS] Data from every NFC extract is compared with application data, and the latter is updated, if needed, to reflect corrections made by NFC. [Web 52] Employee data is updated biweekly from NFC; SF-52 data is complete once signed off and not changeable. [eCalendar] Not defined. [SDMS] Not defined. [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] Not defined [IPIA] Not applicable at this juncture. [SCORP] Not defined.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No non-standard or new technologies are employed.
3b. How does the use of this technology affect customer/employee privacy?	N/A
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	[TMS] TMS uses SSN and employee home address (these data must be in the application document form). Only authorized users can get access to these data. [Flotrack] For authorized users, the system will allow the monitoring of a FLO trainee's status within the training program. Because the system tracks office location and state both within email address and as a separate data field, individuals can be located at the state level. [ORAS] No [Contact Search] Contact Search does not display sensitive information of employees. Information such as phone number, office location, and email address will be helpful to locate an individual. [SMDA] No [IMS] No, other than individuals designated to get supplies from the supply room. [eFSRS] No [Web 52] No [eCalendar] No

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	[SDMS] No [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] No. [IPIA,SCORP] No
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	[TMS] No [Flotrack] No. [ORAS] No [Contact Search] No [SMDA] No [IMS] No [eFSRS] No [Web 52] No [eCalendar] No [SDMS] No [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] No [IPIA, SCORP] No
4c. What controls will be used to prevent unauthorized monitoring?	[TMS] TMS System is intranet application it is supposed to work in trusted boundaries (USDA intranet). [Flotrack] Intranet app, presumably working only within the boundaries of the trusted USDA intranet. Role based authorization limits the data available to individuals. [ORAS] N/A [Contact Search] Contact Search is an intranet application it is supposed to work in trusted boundaries (USDA intranet). [SMDA] SMDA System is an internet application. It is can be accessed only if an eAuthentication ID is assigned by the DSA group. [IMS] System is intranet application it is supposed to work in trusted boundaries (USDA intranet). [eFSRS] System is intranet application it is supposed to work in trusted boundaries (USDA intranet). [Web52] System is intranet application it is supposed to work in trusted boundaries (USDA intranet). [eCalendar] System is intranet application it is supposed to work in trusted boundaries (USDA intranet)

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	[SDMS] System is intranet application it is supposed to work in trusted boundaries (USDA intranet). [EOTS Reporting] See response under EOTS Client/Server Administrative Systems for this question. [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] System is intranet application it is supposed to work in trusted boundaries (USDA intranet) [IPIA] N/A [SCORP] N/A
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	[TMS, Contact Search, IMS, eFSRS, eCalendar, SDMS, WIMS, RTS, SCORP] FSA-7 (Employees Resource Master File) [ORAS, Flotrack, SMDA] FSA – 2 (Farm Records File) [EOTS Reporting] FSA – 10 Investigation and Audit Reports [eWIMS] See response under WIMS Client/Server Administrative Systems for this question. [eRTS] FSA-7 (Employees Resource Master File) [IPIA] Not applicable. This application is an extension of the County Operations Review Program (CORP) Reporting process that is not subject to the privacy act provisions. Information is accessed by State and County code and not by producer name or ID. Information under CORP is subject to the provisions of the Freedom of Information Act.
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	No

3.2 *Focus Administrative Systems (FAS)*

FAS Table 6: Data In The System

DATA IN THE SYSTEM	
1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	[EIS] Customer is Employee. Employee Info: Name, Organization, Pay Plan, Series, Salary, Budget Position Number. Organization Statistics by Race and Gender and Grade. SSNO is stored in database but not displayed by reporting system. [WARMIS] Customer/Employee is DACO, Warehouse Inventory Division. DACO uses the following type of information in the system: Warehouse names, codes, capacity, addresses and quantity; insured and uninsured rates; commodity codes, classes, grades and proteins; state names and codes; agreement type codes; entity names; rates month and year; status codes; and country terminal indicator. [CRS] Customer/Employee is the Deputy Administrator for Farm Programs/Common Processes Section (DAFP/CP). Data in system is used to perform farm crop and analysis.
2a. What are the sources of the information in the system?	[EIS] Data from National Finance Center (Paypers, Table5B) [WARMIS] Data from Grain Inventory Management System (GIMS) mainframe database system. [CRS] Data from NITC (State Offices data transmitted to mainframe).
2b. What USDA files and databases are used? What is the source agency?	[EIS] User organization database: Sion.foc, Sion.mas Source FSA COUNTY: COEADTL.WP, COEAORG.WP, COEATOT.WP, COEBRAN.FTM,COEDIV.FTM, COEOPDV.FTM,COESGRD.WP,COESGRP.WP COESGRT.WP, SALCOC1.FOC, SALCOC1.MAS, SALCOE1.FOC, SALCOE1.MAS, SALCOE2.FOC, SALCOE2.MAS, SALCOE3.FOC, SALCOE3.MAS SALCOE4.FOC, SALCOE4.MAS, SALCOE5.FOC, SALCOE5.MAS, STATES01.FTM, STATES02.FTM, STATES03.FTM, STATES04.FTM, STATES05.FTM Source FSA Federal: FSAADTL.WP, FSAAORG.WP, FSAATOT.WP, FSABRAN.FTM,FSADIV.FTM, FSAOPDV.FTM,FSASGRD.WP,FSASGRP.WP FSASGRT.WP, SALPERS1.FOC,SALPERS1.MAS S01PERS1.FOC, S01PERS1.MAS

DATA IN THE SYSTEM	
	S02PERS1.FOC, S02PERS1.MAS S03PERS1.FOC, S03PERS1.MAS S05PERS1.FOC, S05PERS1.MAS S06PERS1.FOC, S06PERS1.MAS S07PERS1.FOC, S07PERS1.MAS Source RMA Federal: RMAADTL.WP, RMAAORG.WP, RMAATOT.WP, RMABRAN.FTM,RMADIV.FTM, RMAOPDV.FTM,RMASGRD.WP,RMASGRP.WP RMASGRT.WP, SALRMA1.FOC,SALRMA1.MAS, S01RMA1.FOC, S01RMA1.MAS, S02RMA1.FOC, S02RMA1.MAS S03RMA1.FOC, S03RMA1.MAS, S04RMA1.FOC, S05RMA1.MAS Source FAS Federal: FASADTL.WP,FASAORG.WP,FASATOT.WP, FASBRAN.FTM,FASADIV.FTM, FASOPDV.FTM,FASSGRD.WP,FASSGRP.WP FASSGRT.WP, SALFAS1.FOC, SALFAS1.MAS, S01FAS1.FOC, S01FAS1.MAS, S03FAS1.FOC, S03FAS1.MAS S04FAS1.FOC, S04FAS1.MAS, S05FAS1.FOC, S05FAS1.MAS, S06FAS1.FOC, S06FAS1.MAS S07FAS1.FOC, S07FAS1.MAS, S08FAS1.FOC, S08FAS1.MAS [WARMIS] Data comes from GIMS views: County, Contract, Entity, Exams, Inventory Loan, Inventory Own, Warehouse Location, Offer Rates, Rates, Warehouse Location, Warehouse [CRS] Data comes from msp905.mmbc1001.
2c. What Federal Agencies are providing data for use in the system?	[EIS] USDA-National Finance Center [WARMIS,CRS] USDA-KC
2d. What State and Local Agencies are providing data for use in the system?	[EIS,WARMIS,CRS] N/A
2e. From what other third party sources will data be collected?	[EIS,WARMIS,CRS] N/A
2f. What information will be collected from the customer/employee?	[EIS,WARMIS,CRS] No data is collected from customer or employee.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	[EIS,WARMIS,CRS] N/A
3b. How will data be checked for completeness?	[EIS] Human Resources Division (HRD) checks for accuracy or customer notes a discrepancy and reports it to HRD. NFC biweekly downloads provide updates

DATA IN THE SYSTEM	
	to correct any data problems. [WARMIS] user makes comparison to info received from other sources. [CRS] User contacts State Offices.

FAS Table 7: Access To The Data

ACCESS TO THE DATA	
1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	[EIS] Users with/without Sensitive and EEO Statistics, Users with all agency access, one agency, Division access only. System allows sensitive and/or non-sensitive access privilege. One system administrator and one backup system administrator [WARMIS,CRS] User, Administrators and Developer will have access to the data.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	[EIS] Employee requesting access must have supervisory approval and supervisor must dictate level of access required. No request is submitted to FSA ISO. [WARMIS,CRS] Employee requesting access must have supervisory approval. No request is submitted to FSA ISO.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	[EIS] Access is based on organization database privilege to view data. The system is Client Server and does not use Eauth. [WARMIS] The data is for DACO view and the users have access to all the data on the system. [CRS] The data is for DAFP/CP view and the users have access to all the data on the system.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	[EIS] User access is limited by organizational level of access. If user access is limited to an agency or organization structure then that is the only data the user is allowed to see. [WARMIS] The system administrator grants the permission for users. [CRS] User is granted to have access to system.
5a. Do other systems share data or have access to data in this system? If yes, explain.	[EIS] Yes, Quarterly, the data is copied and merged with Farm Credit Loan data that is downloading from Kansas City Mainframe. Data is merged by ssno to produce new data file that is uploaded to Kansas City Mainframe [WARMIS,CRS] No
5b. Who will be responsible for protecting the privacy rights of the customers and	[EIS] EIS system and EMSO. DAA has the ultimate responsibility. [WARMIS,CRS] N/A

ACCESS TO THE DATA	
employees affected by the interface.	
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	[EIS] FSA, RMA, FAS [WARMIS,CRS] No
6b. How will the data be used by the agency?	[EIS] FSA, RMA, FAS Management accesses Employee Workforce Data counts & EEO statistics. [WARMIS] N/A [CRS] N/A
6c. Who is responsible for assuring proper use of the data?	[EIS] HRD is responsible for proper use of data. [WARMIS] N/A [CRS] N/A

FAS Table 8: Attributes Of The Data

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?	[EIS,WARMIS,CRS] Yes. See section 2.2
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	[EIS] System creates counts of employee data by criteria provided by HRD and displays employee names within each organizational structure. Organization structure are aggregated to speed data retrieval [WARMIS] System completely refreshes once a week with new data. [CRS] System data is overwritten monthly.
2b. Will the new data be placed in the individual's record (customer or employee)?	[EIS] HRD provides ceiling levels for FSA only and these figures are updated in the code not the database. Organization aggregation is stored with each individual database. [WARMIS,CRS] No
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	[EIS] System counts are created on the fly and not stored. Counts by race and sex are grouped by grade ranges or occupational series and not at individual level. [WARMIS,CRS] No
2d. How will the new data be verified for relevance and accuracy?	[EIS] Data is downloaded biweekly from NFC. HRD has provided rules for calculating employee counts by type of position (Fulltime,PartTime,Co-op,Other) [WARMIS] User compares results to reports and/or queries from KC. [CRS] User compares results to other reports and/or contact State Offices.

ATTRIBUTES OF THE DATA	
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	[EIS] Only employee counts are consolidated and only authorized users can access the system. [WARMIS,CRS] Database access is authorized by supervisory approval only.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	[EIS] Data that is downloaded is deleted after being loaded to database. Databases are encrypted and password protected. Only authorized database users can access the system and view data. [WARMIS] Access is based on log on id, which is only given to those whom access the system. [CRS] No consolidation
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	[EIS] System provides reports based on organization drill down to the individual level, no queries are allowed. [WARMIS] Canned reports are created. Data can not be retrieved by personal identifier. [CRS] System provides reports and no queries are allowed.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	[EIS,WARMIS,CRS] none
4c. How are the effects to be mitigated?	[EIS,WARMIS,CRS] N/A

FAS Table 9: Maintenance Of Administrative Controls

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	[EIS] This system is only used by upper management, HRD, Budget users who deal with Workforce summary data. [WARMIS] This system is only used by Managers of DACO [CRS] System only accessed by user or DBA.
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?	[EIS] Data is accessed centrally by FSA, and RMA users. Data is copied to FAS network on a biweekly basis as soon as download is completed. [WARMIS,CRS] N/A
2b. Explain any possibility of disparate	[EIS] System is an internal legacy system

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
treatment of individuals or groups.	approximately 16 years old and no further updates are planned. A possible rewrite to the web is being considered. [WARMIS,CRS] N/A
2c. What are the retention periods of data in this system?	[EIS] All historical data is retained by pay period external to the system. System is backed up on a network drive nightly and weekly. [WARMIS] System is completely refreshed weekly [CRS] Retention period is 1 month.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	[EIS] N/A [WARMIS] System is completely refreshed weekly [CRS] Data is overwritten monthly.
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?	[EIS] Data is updated bi-weekly from NFC. NFC and HRD and user's review determine the accuracy of data. [WARMIS,CRS] User makes comparison.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	[EIS,WARMIS,CRS] No
3b. How does the use of this technology affect customer/employee privacy?	[EIS,WARMIS,CRS] N/A
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	[EIS,WARMIS,CRS] No
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	[EIS,WARMIS,CRS] No
4c. What controls will be used to prevent unauthorized monitoring?	[EIS, WARMIS,CRS] N/A
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	[EIS] USDA/FSA – 6 County Personnel Records; USDA/FSA – 7 Employee Resources Master File [WARMIS] USDA/FSA-2 – Farm Records File [CRS] USDA/FSA-2 – Farm Records File
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	[EIS, WARMIS,CRS] No. Data is not being modified.

3.3 Client/Server Administrative Systems (CSAS)

CSAS Table 10: Data In The System

DATA IN THE SYSTEM	
1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	[WIMS] Customer/Employee: DACO, Warehouse Inventory Division uses the following type of information in the system: Warehouse names, codes, capacity, addresses and quantity; rates handling and storage; commodity codes, classes, grades and proteins; state names and codes; agreement type codes; entity names; license numbers; exams; examiner names; dates; crop years; bale outstanding; cotton types and counts; and loan maturity dates. [RTS] Customer: Provides mechanism to manage and regulate USDA specific federal regulations. Other: Regulation information is stored in database tables: Regulation number, location, overdue regulations, active regulations [EOTS] Access restricted to security type "Confidential" and Managers only for Customer : Producer Last Name, First Name, State, City, County (Data is collected on Audits, Investigations and Hotline Complaints subsystems) Access restricted to security type "Confidential" and to Managers only for Employee: Employee Last Name, First Name, State, City, County(Data is collect on Investigations and Hotline Complaints subsystems)
2a. What are the sources of the information in the system?	[WIMS] Exam: Data comes from KC SQL Server Matterhorn License: Data comes from GIMS Processed Commodities: KC PCIMS Warehouse Rates: Data comes from GIMS Cotton and Cotton Status: Data comes from KC DB2 MKTPD [RTS] Information comes from within USDA [EOTS] Data in input from Office of Inspector General, General Accounting Office and also from Deputy Administrators or State Executive Directors
2b. What USDA files and databases are used? What is the source agency?	[WIMS] Exam: Data comes from KC SQL Server Matterhorn. Database KCCOWLED tables are WLEDentity; WLEDexam and WLEDEmployee License: Data comes from GIMS Mainframe views: MFGIMV1E and MFGIMV2E

DATA IN THE SYSTEM	
	Processed Commodities: Data comes from KC PCIMS views: MFWHSV1E and MFWHSV3E Warehouse Rates: Data comes from GIMS views: County, Contract, Entity, Exams, Inventory Loan, Inventory Own, Warehouse Location, Offer Rates, Rates, Warehouse Location and Warehouse. Cotton Status and Cotton data on KC NITC mainframe in DB2. Tables are KTCOTT_BALE, KTCOTT_LOAN, .KTCOTT_PRPS_WHS_RT, KTCOTT_PRPS_WHTAR, KTCOTT_WHSE_RATE and KTCOTT_WHSE_TARF. [RTS] *Subsystem Exam: Data comes from KC Sybase07 server* *Database REGS* [EOTS] FSA source agency of EOTS Sql Database. EOTS.dll, EOTS_SQL.exe
2c. What Federal Agencies are providing data for use in the system?	[WIMS] USDA/FSA [RTS] USDA/FSA [EOTS] Information is received from Office of Inspector General and General Accounting Office
2d. What State and Local Agencies are providing data for use in the system?	[WIMS,RTS] N/A [EOTS] FSA State Executive Directors
2e. From what other third party sources will data be collected?	[WIMS, RTS, EOTS] N/A
2f. What information will be collected from the customer/employee?	[WIMS,RTS] None [EOTS] Customer : Producer Last Name, First Name, State, City, County (Collected in Audits, Investigations and Hotline Complaints subsystems) Employee: User ID (for Audit Trail Log) Last Name, First Name, State, City, County(Collected for Investigations and Hotline Complaints subsystems)
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	[WIMS, RTS] N/A [EOTS] Employee enters data enter from documentation; System validates data based on business rules. Pick lists are available throughout most of the EOTS system to limit user input errors.
3b. How will data be checked for completeness?	[WIMS] Users make comparison to other received sources. [RTS] Users make comparison to other received sources. [EOTS] Required fields, regular expressions and error messages are displayed appropriately. Spell Checker is used for all text box input. Administrator/Managers review reports for completeness.

CSAS Table 11: Access To The Data

ACCESS TO THE DATA	
1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	[WIMS] Users, Developers, System Administrators will have access. [RTS] Users, Developers, System Administrators will have access. Application account *DB account) has restricted access to the application DB. DB administrator (DB objects) – full access [EOTS] Administrators, Managers, Members, DBA
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	[WIMS] Employee requesting access must have supervisory approval. The request is usually in writing via email and their computer has to be configured for the application. No procedure is in place for tracking and deleting users except for at the USDA\FSA level. Former users who left were prevented access to the system from the agency level. [RTS] Employee requesting access must have supervisory approval. [EOTS] User access is based on roles for, subsystem access level, field level permissions, contact levels. Criteria and controls regarding access are documented in user requirements.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	[WIMS] The data is for DACO view and the users have access to all the data on the system. [RTS] Users have access to all data in system. [EOTS] User access is restricted by access role (Manager, Member, Admin); Subsystem Access(Audits, Investigations, Hotline Complaints and GAO); Contact Level (Organization hierarchy); Field permission level (Confidential, Restricted, Non-Restricted and Public) is checked against the following fields :Related Reports, Location, Producer Last Name, First Name, State, County, City, ORAS History Date, ORAS History Notes.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	[WIMS] The system administrator grants the permission for users. [RTS] N/A [EOTS] Passwords are encrypted. Only users with valid ID and password are allowed in the database, inactive users are disabled. Role base security is enforced and restricts access as noted in item 3.
5a. Do other systems share data or have access to data in this system? If yes, explain.	[WIMS] No [RTS] No [EOTS] There is a web reporting tool. Access is

ACCESS TO THE DATA	
	restricted to authorized user by roles.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	[WIMS] N/A [RTS] N/A [EOTS] EOTS system and ORAS users. Usually the DAA has the ultimate responsibility
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	No
6b. How will the data be used by the agency?	N/A
6c. Who is responsible for assuring proper use of the data?	N/A

CSAS Table 12: Attributes Of The Data

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. See section 2.2
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	[WIMS] Yes [RTS] Yes [EOTS] No
2b. Will the new data be placed in the individual's record (customer or employee)?	[WIMS] No [RTS] No [EOTS] No
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	No
2d. How will the new data be verified for relevance and accuracy?	[WIMS] Users make comparison to other received sources. [RTS] Users make comparison to other received sources. [EOTS] Business rule verification
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	[WIMS] All data is deleted from tables before data is loaded except for the Current and Tariff Rate tables in the subsystem Cotton. [RTS] Application needs a secure logon ID and a password to access the data. [EOTS] No. Subsystems are role based.
3b. If processes are being consolidated,	[WIMS] Access is based on log on id, allowing only

ATTRIBUTES OF THE DATA	
are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	authorized users to access the system. [RTS] Access is based on log on id, allowing only authorized users to access the system. [EOTS]. Access is controlled by roles and subsystem privileges.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	[WIMS] Pre-defined reports are automatically created. Data can not be retrieved by personal identifier. [RTS] Pre-defined reports are automatically created. Data can not be retrieved by personal identifier. [EOTS] Each record in the database has an identifier and retrieves by a case subsystem number.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	No known impact.
4c. How are the effects to be mitigated?	No known impact.

CSAS Table 13: Maintenance Of Administrative Controls

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	[WIMS] Access has only been permitted to users of DACO to generate reports and system administrators to maintain system. [RTS] N/A [EOTS] System provides short key, buttons, and web reporting is 508 compliant.
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?	[WIMS] N/A [RTS] N/A [EOTS] All data storage occurs in one site. Web based intranet access is for reporting only.
2b. Explain any possibility of disparate treatment of individuals or groups.	[WIMS] N/A [RTS] N/A [EOTS] N/A
2c. What are the retention periods of data in this system?	[WIMS] Warehouse Rates, License and Exams retention period is weekly. Processed Commodities retention period is monthly. Cotton Status data retention period is daily.

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	Cotton doesn't have a data retention period except for the Offer table data is deleted annually. [RTS] Currently the data is maintained indefinitely. There are plans about archiving data which may be addressed during new release of the application. Data backup is done regularly for this database. [EOTS] The data records are maintained for 5 years after closure. Database is backed up nightly and weekly based on our Database Administrative processing.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	[WIMS] No procedure documented, but the system administrators run system programs to delete data which are part of the process for updating system. [RTS] Stored procedures are executed to delete data. [EOTS] Five years after record closure the system mark records deletion, user confirms batch deletions and removes them from the system. Retention procedures are part of user 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?	[WIMS] Users generate reports for analysis. [RTS] Users generate reports for analysis. [EOTS] Data in the database is reviewed for accuracy; actions are taken and recorded on all open records until they are closed. Reports are printed and reviewed by ORAS for accuracy.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No
3b. How does the use of this technology affect customer/employee privacy?	N/A
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No
4c. What controls will be used to prevent unauthorized monitoring?	[WIMS] N/A [RTS] N/A [EOTS] Only a small number of users are authorized to access this intranet system, and field level permissions are in place to restrict access to confidential, restrictive, non-restrictive and public data.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	[WIMS] FSA-2 Farm Records Systems [RTS] FSA – 7 Employee Records Resource Master File [EOTS] FSA – 10 Investigation and Audit Reports

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

3.4 WDC Former IPUSO Applications

WDC Former IPUSO Applications Table 14: Data In The System

DATA IN THE SYSTEM	
1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	[Accessions] Captures descriptions of type of file to be stored at the National Archives. Employee Name only. [Non-PO Tracking] Tracks purchases employees request to perform their duties. [SF-39] Input and gather information for vacancy announcement timeframes to meet standards. [PTS] Employees and vendors [WIS] Employee and Vendors [RFA] All users [TAL] Customer: Kansas City Director and Division level secretaries. Information type: Employee names, destinations, dates, amounts of travel. [YMTP] System data is used to provide career information and guidance to employees interested in improving their work skills and enhancing their carriers. [SF-52] System data is used to generate metrics and reports for different types of actions requested by the program areas.
2a. What are the sources of the information in the system?	[Accessions] Data is input by users from form SF-135. [NON-PO TRACKING] Various catalogs the Procurement division provides, sometimes on-line. [SF-39] When a request is received to fill a position until vacancy closes. [PTS] Data input by the users and NFC [WIS] Data input by the users [RFA] Type of work FSA does [TAL] Data comes from the employee and NFC documents AD616 & 202. [YMTP] User inputs all data. [SF-52] User inputs all data.
2b. What USDA files and databases are used? What is the source agency?	[Accessions] Access db [NON-PO TRACKING] Access db [SF-39] Access db [PTS] Files and databases [WIS] Individual files and databases [RFA] Databases. eAuth, RFA, IMBED [TAL] FSA NFC AD616 & 202 documents and shared DB.

DATA IN THE SYSTEM	
	[YMTP] Youth Mentoring and Tutoring Program is Client/Server. [SF-52] MS Access and Visual Basic.
2c. What Federal Agencies are providing data for use in the system?	[Accessions] None. [NON-PO TRACKING] GSA and catalogs. [SF-39] FSA, RD, NRCS, FS [PTS] FSA, RMA, NFC [WIS] FSA, RMA, OCIO, WDC awards [RFA] FSA [TAL] None [YMTP] None [SF-52] None
2d. What State and Local Agencies are providing data for use in the system?	[Accessions] All FSA offices. [NON-PO TRACKING] Business supply stores. [SF-39] None [PTS] None [WIS] 2600 counties and agencies and all local subsidiaries [RFA] None [TAL] None [YMTP] None [SF-52] None
2e. From what other third party sources will data be collected?	[Accessions] None. [NON-PO TRACKING] None. [SF-39] N/A [PTS] N/A [WIS] N/A [RFA] None [TAL] N/A [YMTP] None [SF-52] None
2f. What information will be collected from the customer/employee?	[Accessions] Employee name. [NON-PO TRACKING] Supplies they require. [SF-39] None [PTS] Vendor, product and supply information [WIS] Supplies they require.

DATA IN THE SYSTEM	
	[RFA] None [TAL] Employee: name, destinations, dates, and travel amounts. [YMTP] Primary purpose of application is not data collection, but informational purposes as to what training, classes are available. [SF-52] N/A
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	[Accessions] N/A [NON-PO TRACKING] Could manually call the store for accurate cost. [SF-39] N/A [PTS] Buyers confirm availability and pricing directly from the vendors [WIS] Perform enquires into the databases [RFA] All validation done internally [TAL] NFC [YMTP] None [SF-52] None
3b. How will data be checked for completeness?	[Accessions] Self check [NON-PO TRACKING] Db has validations built-in. [SF-39] Business rules of the application. [PTS] Buyers check data for completeness prior to conclusion of the buy [WIS] Business rules of the application [RFA] N/A [TAL] Required fields validation [YMTP] Validations are pre-defined. [SF-52] Validations are pre-defined.

WDC Former IPUSO Applications Table 15: Access To The Data

ACCESS TO THE DATA	
1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	[Accessions] There are six users, one administrator, and one Manager. [NON-PO TRACKING] System administrators, developers and Director. [SF-39] The users and Managers [PTS] Users, Managers, System Administrators [WIS] Users, Managers, System Administrators [RFA] Admin for running job. All users [TAL] Kansas City Directors, Office Chiefs &

ACCESS TO THE DATA	
	Secretaries [YMTP] Users have access by using role-based views. [SF-52] Human Resources Division, KC , users, managers, and system administrators are role based.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	[Accessions] Password protected. [NON-PO TRACKING] Password protected. [SF-39] Access to data is determined by roles built into the application. [PTS] Access to data is determined by roles built into the application. [WIS] As needed basis [RFA] Through Managers and eauth validation [TAL] Limited Availability and Usage – Supervisor Approval. [YMTP] Access to data is determined by roles built into the application. [SF-52] Access to data is determined by roles built into the application.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	[Accessions] Users have access to all data in system. [NON-PO TRACKING] Based on business rules, users are restricted. [SF-39] All data. [PTS] Access to data is determined by roles built into the application. [WIS] Based on business rules, users are restricted. [RFA] Different levels of authority decided by the managers. Restricted [TAL] User access is restricted by access role [YMTP] Access to data is restricted and is based on user permission set roles. [SF-52] Access to data is restricted and is based on user permission set roles.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	[Accessions] Authorized users. [NON-PO TRACKING] Role-based security check [SF-39] Data is only on users computers that have access. [PTS] Only Authorized users can get to it. [WIS] Authorized users.

ACCESS TO THE DATA	
	[RFA] Access through eauth. Again screened by the people who run the job [TAL] Password Protected [YMTP] Access to data is restricted and is based on user permission set roles. [SF-52] Access to data is restricted and is based on user permission set roles.
5a. Do other systems share data or have access to data in this system? If yes, explain.	No
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	N/A
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	[Accessions] National Archives will retain the data files. [NON-PO TRACKING] No. [SF-39] No [PTS] Federal [WIS] Federal, state, local [RFA] No [TAL] No [SF-52] No [YMTP] No
6b. How will the data be used by the agency?	[Accessions] Storage only. [NON-PO TRACKING] This is the first step towards requisitioning supplies. [SF-39] Reporting metrics and standards. [PTS] This is the first step towards requisitioning supplies. [WIS] [RFA] Provide services for the customers [TAL] Secretaries and Managers use this source in tracking the travel budget [SF-52] The data will be used by HR for tracking tasks and generating reports to management. [YMTP] No
6c. Who is responsible for assuring proper use of the data?	[Accessions] Authorized users. [NON-PO TRACKING]Authorized users. [SF-39] The users [PTS] Buyers [WIS] Administrators [RFA] Staff from IPUSO

ACCESS TO THE DATA	
	[TAL] Users [SF-52] Application and authorized users. [YMTP] Information is used to advance employees skills.

WDC Former IPUSO Applications Table 16: Attributes Of The Data

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. See section 2.2
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No
2b. Will the new data be placed in the individual's record (customer or employee)?	N/A
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	N/A
2d. How will the new data be verified for relevance and accuracy?	N/A
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	N/A
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	N/A
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	[Accessions]Stored on a shared drive with restrictive access. [NON-PO TRACKING] Business rules are in place. No. [SF-39] Data is manually input [PTS] No [WIS] Data is manually input [RFA] User id or application name or division [TAL] Data cannot be retrieved by personal identifier. [SF-52] Data is retrieved through application screens and event searches. [YMTP] Access to data is verified by system based on user attributes and roles.

ATTRIBUTES OF THE DATA	
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	none
4c. How are the effects to be mitigated?	N/A

WDC Former IPUSO Applications Table 17: Maintenance Of Administrative Controls

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	[Accessions] N/A [NON-PO TRACKING] N/A [SF-39] N/A [PTS] As designed it will ensure equitable treatment to customers and employees [WIS] Information is only for government employees [RFA] N/A [TAL] N/A [YMTP] All employees within a given role are treated equally. [SF-52] System is designed per USDA guidelines that ensure equitable treatment of employees.
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?	[Accessions] N/A [NON-PO TRACKING] N/A [SF-39] N/A [PTS] N/A [WIS] access through authorized application [RFA] N/A [TAL] N/A [SF-52] Only operated at one site [YMTP] N/A
2b. Explain any possibility of disparate treatment of individuals or groups.	None known
2c. What are the retention periods of data in this system?	[Accessions] Historical data is retained by National Archives.

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
	[NON-PO TRACKING] At least one year. [SF-39] Three years [PTS] Historical data is retained indefinitely [WIS] Retained information for about 10 years. Backup tapes are retained for not more than a year. [RFA] All historical information is stored. [TAL] Currently the data is maintained indefinitely. [YMTP] All historical data is retained. [SF-52] All historical data is retained.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	[Accessions] N/A [NON-PO TRACKING] Business rules define the procedures. [SF-39] Policy is to delete any year after three. [PTS] N/A [WIS] Policy in place to delete after the above period [RFA] N/A [TAL] Not defined, but archived [SF-52] Not defined by the business owner. [YMTP] Not defined by business owners.
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?	[Accessions]N/A [NON-PO TRACKING]Not defined by business owner. [SF-39] None defined. [PTS] Reviewed by the buyer [WIS] Number of demands and frequencies [RFA] All data has timestamp [TAL] Users generate reports for review [YMTP] Not defined. [SF-52] Not defined.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No
3b. How does the use of this technology affect customer/employee privacy?	N/A
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No
4c. What controls will be used to prevent	[Accessions]Password Protected. [NON-PO TRACKING]Password Protected.

MAINTENANCE OF ADMINSTRATIVE CONTROLS	
unauthorized monitoring?	[SF-39] Business rules. [PTS] Limited access and identified roles [WIS] Password protected [RFA] N/A [TAL] N/A [SF-52] System is intranet application it is supposed to work in trusted boundaries (USDA intranet) [YMTP] System is intranet application, it is supposed to work in trusted boundaries (USDA intranet)
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	USDA/FSA-2 USDA/FSA-3 USDA/FSA-5 USDA/FSA-6
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	Possibly if the modification results in data, record storage location, or routine use that is not covered by the SORN identified above.

PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM

I have carefully assessed the Privacy Impact Assessment for the

Consolidated Administrative Systems – Washington, DC (CAS-WDC)
(System Name)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

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.

____

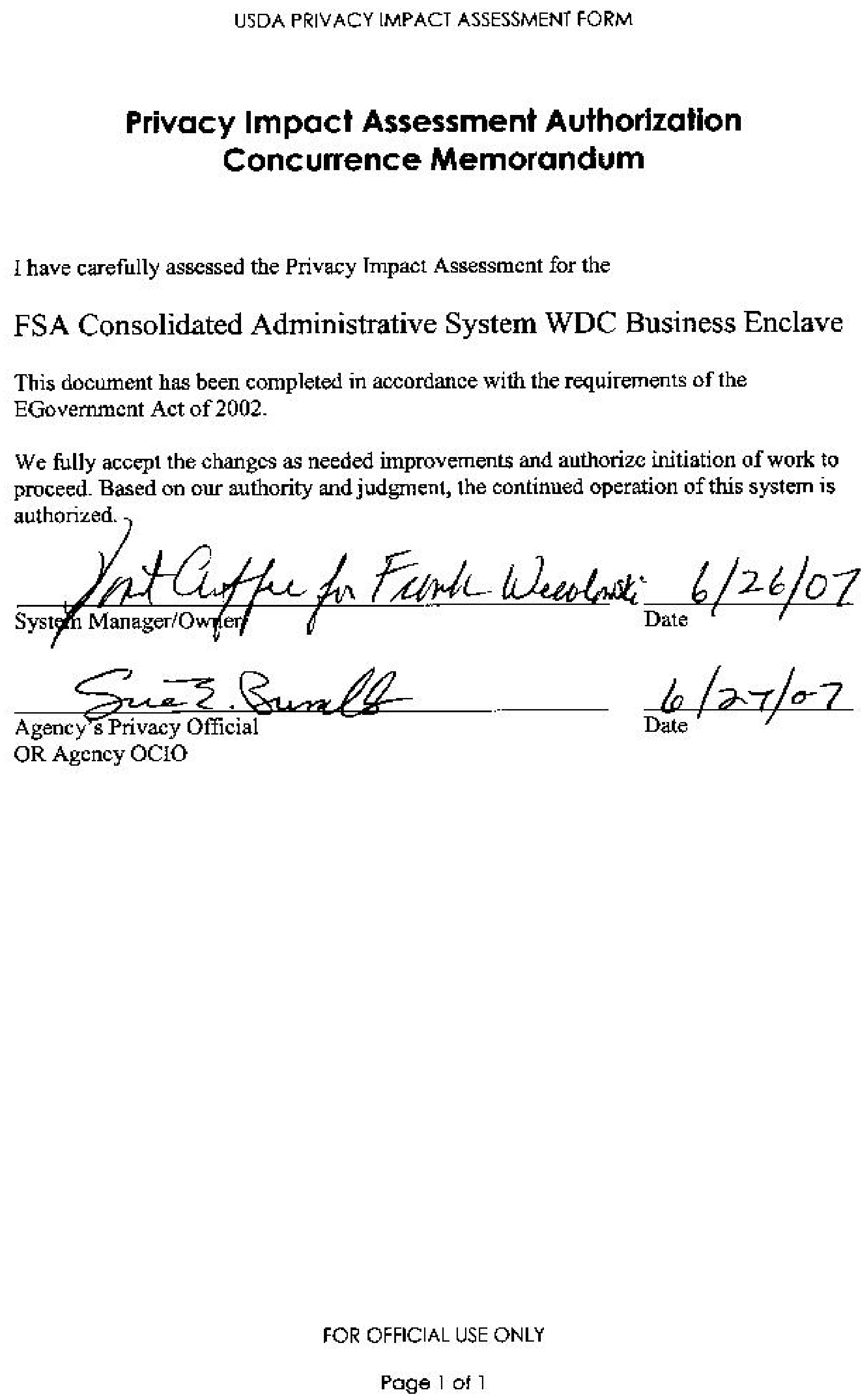
System Manager/Owner OR Project Representative OR Program/Office Head	Date

____

Agency's Chief FOIA officer OR Senior Official for Privacy OR Designated privacy person	Date

____

Agency CIO	Date



USDA PRIVACY IMPACT ASSESSMENT FORM

Privacy Impact Assessment Authorization Concurrence Memorandum

I have carefully assessed the Privacy Impact Assessment for the

FSA Consolidated Administrative System WDC Business Enclave

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

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/Owner — Date 6/26/07

Agency's Privacy Official
OR Agency OCIO — Date 6/27/07

FOR OFFICIAL USE ONLY

Page 1 of 1