Privacy Impact Assessment (PIA)

Telework Management System (TMS)

Revision: *1.06*

Farm Service Agency

Date: *July 24, 2009*

Document Information

Owner Details	
Name	Vivek Agnihotri
Contact Number	(202) 690-0714
E-mail Address	Vivek.Agnihotri@wdc.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.01	July 6, 2009	D.Brizendine ISO	Initial version.
1.02	July 6, 2009	D.Brizendine ISO	Populated Sections 3,4,5
1.03	July 14, 2009	Scott Tanos	
1.04	July 20, 2009	D.Brizendine ISO	Updated System Owner information
1.05	July 23, 2009	Rani Agnihotri	Updated incomplete answers
1.06	July 24, 2009	D.Brizendine	Updated responses for 24, 25, 26, 26.1; Document review

Table of Contents

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 Telework Management System 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 System Information

System Information	
Agency:	Farm Service Agency (FSA)
System Name:	Telework Management System
System Type:	☐ Major Application ☐ General Support System ☒ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	Telework Management System (TMS) automates the telework application process, telework reporting, and tracking of application routing and service request fulfillment.
Who owns this system? (Name, agency, contact information)	Vivek Agnihotri (202) 690-0714 Vivek.Agnihotri@wdc.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information System Security Program Manager (ISSPM) U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250 (202) 720-2419 brian.davies@wdc.usda.gov
Who completed this document? (Name, agency, contact information)	Rani Agnihotri (202) 690-0458 Rani.Agnihotri@wdc.usda.gov Thomas Berg (202) 720-2680 Thomas.Berg@wdc.usda.gov

3 Data Information

3.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Application is used by FFAS employees to submit and receive telework approval from their supervisors. Data is used by HRD to provide mandated OPM telework reports.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☒ Yes ☐ No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	Executive Order #9397
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No
4	Sources of the data in the system.	Telework requests are entered by employees and additional data is provided by National Finance Center (NFC) downloads. NFC-FFAS data is downloaded from NFC to Shared. Data is retrieved from Shared by using customized views.
4.1	What data is being collected from the customer?	Phone number, email address, User Interface preferences and telework residences.
4.2	What USDA agencies are providing data for use in the system?	Shared DB, FSA
4.3	What state and local agencies are providing data for use in the system?	FFAS (DC and KC)
4.4	From what other third party sources is data being collected?	None
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☒ Yes ☐ No – If NO, go to question 6.

No.	Question	Response
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Required field and regular expression validations, business rules.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Required field and regular expression validations, business rules.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	No data collected outside of the USDA.

3.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	Creation and tracking of telework applications and agreements.
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.
7.1	What are the other purposes?	
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	☒ Yes ☐ No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☒ Yes ☐ No – If NO, go to question 10. Dynamically assigned some additional application-specific user attributes based on existing employee's data (supervisory status, e.g.)
9.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☒ No - These data derived automatically and used per-session basis.
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☒ No

No.	Question	Response
9.3	How will the new data be verified for relevance and accuracy?	Business rule verification
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	Creation and tracking of telework applications and agreements.
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 12.
11.1	What are the other uses?	
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	Role-based controls.
13	Are processes being consolidated?	☐ Yes ☒ No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	

3.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	
14.2	What are the procedures for purging the data at the end of the retention period?	
14.3	Where are these procedures documented?	

No.	Question	Response
15	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?	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.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

3.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☐ Yes ☒ No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	
17.2	Who is responsible for assuring the other agency properly uses the data?	
18	Is the data transmitted to another agency or an independent site?	☐ Yes ☒ No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	
19	Is the system operated in more than one site?	☐ Yes ☒ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	

3.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	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.

No.	Question	Response
21	How will user access to the data be determined?	eAuthentication and Role-based security check.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No eAuthentication and Role-based security check.
22	How will user access to the data be restricted?	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.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No Role-based security check; Release 1.0 – partial display of SSN.

3.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	USDA Privacy Office
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	By contacting John Underwood, Privacy Officer, at john.underwood@kcc.usda.gov & 816.926.6992
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 27. Common FSA incident reporting process. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	

No.	Question	Response
27	Consider the following: Consolidation and linkage of files and systems Derivation of data Accelerated information processing and decision making Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	All employees within a given role are treated equally by the system, based on pre-defined business rules.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	

4 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes ☐ No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	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.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	FSA-7 (Employees Resource Master File)
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

5 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	☐ Yes ☒ No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	

6 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.