



Privacy Impact Assessment for
Fingerprint Identification System (FIS)




**Privacy Impact Assessment Authorization
Memorandum**

I have carefully assessed the Privacy Impact Assessment for the

Fingerprint Identification System

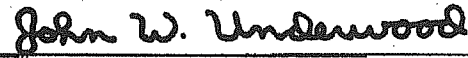
This document has been completed in accordance with the requirements of the E-Government Act of 2002.

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.



Dewayne Brown, ITSD/HOIRC/EMSO,
Information System Owner

4/19/2010
Date



John Underwood, Chief Privacy Officer

4/23/10
Date



Jim Gwinn, ESA CIO

4/28/2010
Date



Privacy Impact Assessment (PIA)

**Fingerprint Identification System
(FIS)**

Revision: 1.04

Farm Service Agency

Date: April 19, 2010





Privacy Impact Assessment for
Fingerprint Identification System (FIS)



Document Information

Business Owner Details	
Name	Jacqueline Whitaker, Director, HRD
Contact Number	(202) 401-0089
E-mail Address	Jacqueline.Whitaker@wdc.usda.gov

Document Revision and History			
Revision	Date	Author	Comments
1.01	April 07, 2010	Anita Trader	Initial version
1.02	April 12, 2010	Anita Trader	Updated Business Owner
1.03	April 15, 2010	Anita Trader	Updated section 2 doc completion
1.04	April 15, 2010	S. Timbrook, ECS	Review document and update to common verbiage. Change Business owner on signature page to information owner.
1.05	April 19, 2010	DeWayne Brown	Reviews document
1.06	04/26/2010	T. Ostrander	Made changes per C. Niffen from John Underwood.



Table of Contents

1	PURPOSE OF DOCUMENT	1
2	SYSTEM INFORMATION	2
3	DATA INFORMATION	3
3.1	Data Collection	3
3.2	Data Use	4
3.3	Data Retention.....	6
3.4	Data Sharing.....	6
3.5	Data Access	7
3.6	Customer Protection.....	7
4	SYSTEM OF RECORD	9
5	TECHNOLOGY	9
6	COMPLETION INSTRUCTIONS.....	10



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 **Fingerprint Identification 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*.



Privacy Impact Assessment for
Fingerprint Identification System (FIS)



2 System Information

System Information	
Agency:	Farm Service Agency
System Name:	Fingerprint Identification System
System Type:	<input checked="" type="checkbox"/> Major Application <input type="checkbox"/> General Support System <input type="checkbox"/> Non-major Application
System Categorization (per FIPS 199):	<input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low
Description of System:	Fingerprint Identification System (FIS) enables FSA staff to electronically capture civil applicant fingerprints and biographical data and to transmit the data to the Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS) via the CAS satellite system as part of the background investigations of new Department employees, political appointees, and contractors.
Information System Owner? (Name, agency, contact information)	Dewayne Brown, ITSD/HOIRC/EMSO U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250 (202) 690-1146 Dewayne.Brown@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)	Anita Trader, ISO DR (from current document information) 816-823-3741 Anita.Trader@kcc.usda.gov



3 Data Information

3.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Fingerprint and biographical data of political appointees, employees, employment applicants, and contractors working on behalf of USDA granted or seeking access to USDA controlled facilities and/or USDA information systems.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and 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.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
4	Sources of the data in the system.	Political appointees, employees, employment applicants, and contractors working on behalf of USDA.
4.1	What data is being collected from the customer?	Name, home address, social security number, telephone number, Email address, race, sex, gender, fingerprint, height and weight.
4.2	What USDA agencies are providing data for use in the system?	None
4.3	What state and local agencies are providing data for use in the system?	None
4.4	From what other third party sources is data being collected?	Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS) response concerning the request for fingerprint inquiry and evaluation.
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?	Data collected from the customer is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data collected from non-USDA sources is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

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?	To support electronically capturing political appointee, employee, employment applicant, and contractor working on behalf of USDA fingerprints and biographical data and to transmit the data to the Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS) via the CAS satellite system as part of the background investigation and suitability adjudication determination process.
7	Will the data be used for any other purpose?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 8.
7.1	What are the other purposes?	N/A
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	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 10.



Privacy Impact Assessment for
Fingerprint Identification System (FIS)



No.	Question	Response
9.1	Will the new data be placed in the individual's record (customer or employee)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
9.3	How will the new data be verified for relevance and accuracy?	The new data is verified by DOJ, for relevance and accuracy by the customer and FSA employee upon entry of the data into the system.
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?	To support electronically capturing political appointee, employee, employment applicant, and contractor working on behalf of USDA fingerprints and biographical data and to transmit the data to the Department of Justice (DOJ) Integrated Automated Fingerprint Identification System (IAFIS) via the CAS satellite system as part of the background investigation and suitability adjudication determination process.
11	Will the data be used for any other uses (routine or otherwise)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 12.
11.1	What are the other uses?	None
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?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	N/A
13	Are processes being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	N/A



3.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?	Paper document is filed in the security folder and maintained indefinitely.
14.2	What are the procedures for purging the data at the end of the retention period?	Manual deletion in the CAS system
14.3	Where are these procedures documented?	The User Manual and OPM Guide to Personnel Record Keeping
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?	Fairness in making determinations is assured because policy requires that the information be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	Data will be shared with partner agencies via service level agreements or Memoranda of Agreements for Contractor security clearances.
17.2	Who is responsible for assuring the other agency properly uses the data?	Each agency has a Security Officer or FOIA Officer/Privacy Act Officer that will promulgate procedures for proper use of data. The Security Officer and FOIA Officer/Privacy Act Officer verify the procedures are followed.
18	Is the data transmitted to another agency or an independent site?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 19.



Privacy Impact Assessment for
Fingerprint Identification System (FIS)



No.	Question	Response
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	Yes - Service Level Agreement; DOJ and Farm Service Agency dated May 14, 2007 - Interconnection Security Agreement: DOJ and OCIO-ITS dated May 10, 2007
19	Is the system operated in more than one site?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	Sites will be independent of each other; however, both sites will use the same User Manual and policies.

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 and System Administrators
21	How will user access to the data be determined?	By System Administrators based on responsibilities and duties .
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
22	How will user access to the data be restricted?	User id and Password protected , Workstation is locked in a secure area
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

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



Privacy Impact Assessment for
Fingerprint Identification System (FIS)



No.	Question	Response
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	FSA National Help Desk at (800)-255-2434 or the Centralized Help Desk at 800-457-3642 or By contacting John W. Underwood, Privacy Officer, at FSA Privacy Act Officer / FSA PII Officer USDA - Farm Service Agency Beacon Facility - Mail Stop 8388 9240 Troost Avenue Kansas City, Missouri 64131-3055 Phone: 816-926-6992 Cell: 816-564-8950 Fax: 816-448-5833 mailto:john.underwood@kcc.usda.gov
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?	<input checked="" type="checkbox"/> Yes – If YES, go to question 27. <input type="checkbox"/> No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	N/A
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)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	Due process procedures are submitted to each customer upon notification of decisions.
28	How will the system and its use ensure equitable treatment of customers?	By providing a centralized and standardized method of processing the information within the system.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 30
29.1	Explain	N/A



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?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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.)?	Name or social security number
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 .)	OPM/GOVT-1 General Personnel Records USDA/FSA-3 Consultants File USDA/FSA-6 County Personnel Records USDA/FSA-7 Employee Resources Master File
30.3	If the system is being modified, will the SOR require amendment or revision?	<input checked="" type="checkbox"/> <input type="checkbox"/> No

5 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	N/A



Privacy Impact Assessment for
Fingerprint Identification System (FIS)



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.