



Privacy Impact Assessment

Fingerprint Identification System (FIS)

Revision: 1.2

USDA Rural Development

Date: October 2008



Document Information

St. Louis Owner Details	
Name	Bonnie Taylor
Contact Number	(314) 457-5541
E-mail Address	bonnie.taylor@stl.usda.gov

Washington DC Owner Details	
Name	Marjorie Beverly
Contact Number	(202) 692-0176
E-mail Address	marjorie.beverly@wdc.usda.gov

Revision History			
Revision	Date	Author	Comments
1.0	20 Oct 2008	Eugene Texter	New Document
1.1	22 Oct 2008	Tom Case	Update new document
1.2	30 Oct 2008	Derrick Wright	Update document with HR PM provided information

Distribution List			
Name	Title	Agency/Office	Contact Information
Bonnie Taylor	St. Louis System Owner	USDA/RD/O&M/HR	bonnie.taylor@stl.usda.gov (314) 457-5541
Brenda Hayes	St. Louis Alternate System POC	USDA/RD/O&M/HR	brenda.hayes@stl.usda.gov (314) 457-5542
Marjorie Beverly	Washington DC System Owner	USDA/RD/O&M/HR	marjorie.beverly@wdc.usda.gov 202-692-0176
Robyne Jackson	Alternate Washington DC System Owner	USDA/RD/O&M/HR	Robyne.jackson@wdc.usda.gov 202-692-0173



Table of Contents

DOCUMENT INFORMATION	ii
TABLE OF CONTENTS.....	iii
1 SYSTEM INFORMATION	1
2 DATA INFORMATION	3
2.1 Data Collection	3
2.2 Data Use	4
2.3 Data Retention.....	5
2.4 Data Sharing.....	5
2.5 Data Access	6
2.6 Customer Protection	7
3 SYSTEM OF RECORD	8
4 TECHNOLOGY	8
5 COMPLETION INSTRUCTIONS.....	8



1 System Information

System Information	
Agency:	USDA Rural Development
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:	<p>The Fingerprint Identification System (FIS) is a satellite system of the Department of Justice (DOJ) Civil Applicant System (CAS) that enables RD staffs to electronically capture civil applicant fingerprints and biographical data and to transmit the data to the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) via the CAS satellite system as part of the background investigations of new Department employees, political appointees, and contractor personnel. The current estimate is that the agency processes 900 fingerprint checks per year.</p> <p>CAS (main system) is located in the Justice Data Center, Washington, D.C. (JDC-W), and makes use of current network integration efforts to interconnect the DOJ and its components with other Federal Departments that utilize the CAS. CAS is operational 24 hours a day, 7 days a week with 99% availability to allow for regular scheduled maintenance.</p> <p>Since any response from IAFIS to a civil applicant submission may contain National Criminal Information Center (NCIC) data, RD must comply with NCIC and USDA security policies as they relate to internal controls, information security, information dissemination, user security, and user training. These policies are described in more detail in the USDA certification and accreditation documents for the CAS satellite system.</p>
Who owns this system? (Name, agency, contact information)	<p>Bonnie Taylor 4300 Goodfellow Blvd. St. Louis, MO 63120 bonnie.taylor@stl.usda.gov 314-457-5541</p> <p>Marjorie Beverly USDA Rural Development 1400 Independence Ave., SW, Mail Stop #0730, Room 1330, Washington, DC 20250 marjorie.beverly@wdc.usda.gov 202-692-0176</p>



Privacy Impact Assessment for Fingerprint Identification System

Who is the security contact for this system? (Name, agency, contact information)	Eugene Texter USDA Rural Development Building 105, FC-44 4300 Goodfellow Boulevard St. Louis, MO 63120 eugene.texter@stl.usda.gov (314) -457-4778 Brenda Dinges USDA Rural Development Building 105, FC-44 4300 Goodfellow Boulevard St. Louis, MO 63120 brenda.dinges@stl.usda.gov (314) -457-4772
Who completed this document? (Name, agency, contact information)	Bonnie Taylor USDA Rural Development 4300 Goodfellow Blvd. St. Louis, MO 63120 bonnie.taylor@stl.usda.gov 314-457-5541



2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Fingerprint and Biographical Data
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.	Executive Orders 10450, 10577, 10865, ,12333, 12968, and, for Social Security Numbers, 9397; Homeland Security Presidential Directive 12; sections 3301, 3302, and 9901 of Title 5 of the United States Code; sections 2165 and 2201 of Title 42 of the United States Code; Chapter 23 of Title 50 of the United States Code; and Title 5, parts 2, 5, 731, 732, 735 and 736 of the Code of Federal Regulations.
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.	
4.1	What data is being collected from the customer?	Name, home address, social security number, race, sex, gender and fingerprint
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?	FBI system sending data back through CAS system
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.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	The information is verified by a driver's license, social security card or a passport; fingerprints are scanned in at the system.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	The information is verified by a driver's license, social security card or a passport



No.	Question	Response
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	The information being sent from the Department of Justice, we assume it's correct.

2.2 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 complete part of the pre-employment process for employees and contractors
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.
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?	We assume the information is correct coming from the DOJ
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?	Send information to Justice and receiving of corresponding report.
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?	N/A



No.	Question	Response
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

2.3 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?	Data will be retained until a verification email from the FBI.
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 Records Retention Regulations
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?	The information is only used for the background investigation process
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

2.4 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.



No.	Question	Response
17.1	How will the data be used by the other agency?	Data will be shared with Dept. of Justice via service level agreements or Memoranda of Agreements for employee/contractor security clearances
17.2	Who is responsible for assuring the other agency properly uses the data?	DOJ is responsible to ensure that the data received from the user (HR) is handled securely while in the possession of DOJ. Overall responsibility for the data rests with the submitting agency (St. Louis and Washington DC HR).
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.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	SLA between RD & DOJ in draft. ISA between RD & DOJ USDA SIGNED 30 Oct 08. Awaiting FBI signature.
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

2.5 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 Appropriate users lists are on file.
21	How will user access to the data be determined?	Those users who only submit data to DOJ will be a user. Those users who have elevated authority to assign users to groups, set up peripherals, etc... will have administrative access.
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?	Password protected and machine is in a locked room
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



2.6 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/HR/DAM/Human Resource Division
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	Bonnie Taylor – STL and Marjorie Beverly – WDC can be contacted via phone and email.
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.	
27	Consider the following: <ul style="list-style-type: none">▪ 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?	All applicant or employee rights, entitlements, laws, rules, and regulations applicable to a manual process for obtaining and determining the acceptability of fingerprint checks continue to apply to the automated process.
28	How will the system and its use ensure equitable treatment of customers?	FIS follows a strict set of procedures that must be complied with when submitting information to the DOJ. DOJ then follows their processes for completing the review and sending of the report. All users are treated exactly the same.
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	



3 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.)?	A Unique Id or the PIN of a person
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)	Nearly all records maintained in HR offices are part of the Office of Personnel Management mandated or regulated government-wide records system. The Office of Personnel Management publishes government-wide records notices in the Federal Register. Fingerprint records are under OPW/GOVT-1 announced in: Federal Register: July 15, 1996 (Volume 61, Number 136).
30.3	If the system is being modified, will the SOR require amendment or revision?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

4 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

5 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.



Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

(System Name)

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

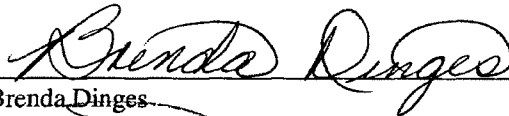
We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.



Allen Hatcher
System Manager/Owner

11/10/08

Date



Brenda Dinges
Designated privacy person

11/10/08

Date



John Distler
Agency DCIO

11/12/08

Date