



**USDA Privacy Impact Assessment (PIA)**  
**Consolidated Financial Management Information System (CFMIS) -**  
**Check Writing System**  
**(CWS)**

**Version 2.0**

**July 2004**

UNITED STATES DEPARTMENT OF AGRICULTURE  
Farm Service Agency (FSA)  
Kansas City, MO 64133

---

DOCUMENT CONTROL

---

**CHANGE RECORD**

<u>Date</u>	<u>Author</u>	<u>Version</u>	<u>Description of Changes</u>
7/9/2004	DSD	1.0	Original Document
7/29/2004	MJG	2.0	Final Document

Table of Contents

<u>Paragraph</u>	<u>Page</u>
1.0 Introduction .....	1
1.1. System Description .....	1
2.0 Privacy Impact Questionnaire .....	1
2.1. System Data .....	1
2.2 Data Access .....	2
2.3. Data Attributes.....	3
2.4. Maintenance of Administrative Controls.....	4
3.0 Summary.....	5

## 1.0 Introduction

The USDA is responsible for ensuring the privacy, confidentiality, integrity, and availability of customer and employee information. Privacy protection is both a personal and fundamental right of USDA customers and employees. Among the most basic of customers and employees' rights is an expectation that USDA will protect the confidentiality of personal, financial, and employment information. Customers and employees also have the right to expect that USDA will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities.

The Privacy Impact Assessment (PIA) is a process used to evaluate privacy concerns and safeguards in computer application systems. The PIA should be initiated in the early stages of the development of a system and completed as part of the required System Life Cycle (SLC) and security reviews. Privacy is one component of system confidentiality and must be considered when requirements are being analyzed and decisions are being made about data usage and system design. A PIA describes the system and its data, any specific privacy concerns, and safeguards established to meet privacy needs. The USDA Privacy Coordinator must be involved in the PIA process.

## 1.1 System Description

The Check Writing System (CWS) is a payment system that falls under the umbrella of FSA's Consolidated Financial Management Information System (CFMIS). CWS issues payments by check for various FSA programs.

## 2.0 Privacy Impact Questionnaire

### 2.1 System Data

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	Customer – Social Security/Tax ID Number, name, address, banking information
2a. What are the sources of the information in the system?	Payment name and address file, banking information, DD
2b. What USDA files and databases are used? What is the source agency?	No files or databases from other agencies are used.

2c. What Federal Agencies are providing data for use in the system?	Any Federal Agency may provide data.
2d. What State and Local Agencies are providing data for use in the system?	N/A
2e. From what other third party sources will data be collected?	N/A
2f. What information will be collected from the customer/employee?	Social Security/Tax ID Number, name, address, banking information
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Eligibility for offset
3b. How will data be checked for completeness?	Field validation

**2.2 Data Access**

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	All county office employees RWO – No resource restrictions State Level – All state level employees National – Read only
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	FSA 13A/0 Standards
3. Will users have access to all data on the system or will the user’s access be restricted? Explain.	Users will have full access to all 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?	Security awareness training

5a. Do other systems share data or have access to data in this system? If yes, explain.	Yes – AJP, DD, EFC, Claims, Receivables
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	CED, SED
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, and Other)?	No other agencies will have access to data in this system.
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

**2.3 Data Attributes**

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No new data will be derived or collected.
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.	Data can be retrieved by check number or issue date.
4b. What are the potential effects on the due process rights of customers and employees of: <ul style="list-style-type: none"> <li>• consolidation and linkage of files and systems;</li> <li>• derivation of data</li> <li>• accelerated information processing and decision making;</li> <li>• use of new technologies.</li> </ul>	None
4c. How are the effects to be mitigated?	N/A

**2.4 Maintenance of Administrative Controls**

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	No violation of EEO
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?	Standard distribution
2b. Explain any possibility of disparate treatment of individuals or groups.	N/A
2c. What are the retention periods of data in this system?	18 months from issue date

<p>2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?</p>	<p>Data is archived to tape, which is maintained for 6 years.</p>
<p>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?</p>	<p>N/A</p>
<p>3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?</p>	<p>No</p>
<p>3b. How does the use of this technology affect customer/employee privacy?</p>	<p>N/A</p>
<p>4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u>? If yes, explain.</p>	<p>No</p>
<p>4b. Will this system provide the capability to identify, locate, and monitor <u>groups of people</u>? If yes, explain.</p>	<p>N/A</p>
<p>4c. What controls will be used to prevent unauthorized monitoring?</p>	<p>N/A</p>
<p>5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.</p>	<p>After research and contact with the Privacy Act Official, the System of Record could not be determined.</p>
<p>5b. If the system is being modified, will the SOR require amendment or revision? Explain.</p>	<p>Undetermined</p>

**3.0 Summary**

This assessment describes the privacy concerns of the CWS infrastructure and its data. As privacy is one of the components of system confidentiality this PIA must be considered anytime requirements are being analyzed and decisions are being made about data usage, security and system design.