



Department of the Interior

Privacy Impact Assessment

Name of Project: Social Services Automated System (SSAS)
**Bureau: Deputy Assistant Secretary-Indian Affairs/Management-
Chief Information Officer**

Date: 03/22/2007

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- **Bureau/office IT Security Manager**
- **Bureau/office Privacy Act Officer**
- **DOI OCIO IT Portfolio Division**
- **DOI Privacy Act Officer**

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

Name of Project: Social Services Automated System (SSAS)
**Bureau: Deputy Assistant Secretary-Indian Affairs/Management-Chief
Information Officer**

Date: 03/22/2007

A. Contact Information

1.) Who is the person completing this document? (Name, title, organization and contact information).

Stephanie Birdwell
Chief Human Service Division
1849 C.Street NW, MS-4513-MIB
Washington, DC 20240

2.) Who is the Business Owner?

Jerry Gidner
Deputy Director of Indian Services
1849 C Street Rm 4513
Washington DC, 20240
(202) 513-7640

3.) Who is the System Owner?

Sanjeev Bhagowalia
Deputy Assistant Secretary-Indian Affairs/Management
Chief Information Officer
Assistant Secretary-Indian Affairs
202-208-0437

4.) Who is the System Manager for this system or application? (Name, organization, and contact information).

Gil Wake
Director, Office of Information Operations
Office of the Chief Information Officer
703-735-4200

5.) Who is the IT Security Manager who reviewed this document? (Name, Organization, and contact Information).

Joan Tyler
Director, Office of Information Security and Privacy
Office of Chief Information Officer
703-735-4387

6.) Who is the Bureau/Office Privacy Act Officer who reviewed this document? (name, organization, and contact information).

Bob Harnage
Director, Office of Information Policy
Office of the Chief Information Officer
703-735-4413

7.) Who is the Reviewing Official?

(According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Sanjeev Bhagowalia
Deputy Assistant Secretary-Indian Affairs/Management
Chief Information Officer
Assistant Secretary-Indian Affairs
202-208-0437

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual¹?

(If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300 and with the IT Security C&A documentation).

Yes

c. Is the information about employees?

(If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation)

No

2) What is the purpose of the system/application? The system produces payments to eligible clients of the social services program.

3) What legal authority authorizes the purchase or development of this system/application? The Synder Act. {25 U.S.C.A. 13 et seq.}

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

C. DATA in the SYSTEM:

- 1) **What categories of individuals are covered in the system?** Recipients of social services financial assistance
- 2) **What are the sources of the information in the system?**
Financial Assistance and Social Services Program Form.
 - a. **Is the source of the information from the individual or is it taken from another source?** The individual
 - b. **What Federal agencies are providing data for use in the system?** The Bureau of Indian Affairs
 - c. **What Tribal, State and local agencies are providing data for use in the system?** Only select tribes are participating and this number varies depending upon the status of their contract and whether they have the resources and expertise to use automated systems.
 - d. **From what other third party sources will data be collected?**
None from employees, individual applicants supply information using OMB approved form, OMB Control # 1076-0017.
 - e. **What information will be collected from the employee and the public?** None of the information comes from employees, but only from the public.
- 3) **Accuracy, Timeliness, and Reliability**
 - a. **How will data collected from sources other than DOI records be verified for accuracy?** Social workers follow up and check sources to ensure the sources of data are in agreement and update when necessary.
 - b. **How will data be checked for completeness?** See a above
 - c. **Is the data current? When applicants come for services, social workers verify that the information on form is correct.**
 - d. **Are the data elements described in detail and documented?** Yes, in case records for recipients. **Case workers follow up on recipient's progress.** See C2a above

D. 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, the data is used for making payments to eligible recipients. The data helps the social worker determine what resources and the amounts that the recipient can receive.
- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?** No
- 3) **Will the new data be placed in the individual's record?**
Any new data received about the individual is placed in the individual's record, but the new data is not the result of manipulating current data.
- 4) **Can the system make determinations about employees/public that would not be possible without the new data?** No, and it does not effect employees, but does contain status of the application and on individual's eligibility for assistance.
- 5) **How will the new data be verified for relevance and accuracy?** No new data created and the security plan and guidance on security is issued.
- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?** The data is restricted in it use and accessibility.
- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Accessibility is restricted
- 8) **How will the data be retrieved?** It is retrieved by case number
- 9) **What kinds of reports can be produced on individuals?** Payment schedules are produced so that individuals obtain payments. Only local agency personnel have access. Employees with access have passwords to control who access to data on clients.
- 10) **What opportunities do individuals have to decline to provide information .** The applicants supply data for eligibility purposes the form explains the limits of use for Privacy Act purposes.
The applicants sign a statement on the form indicating they understand that the information supplied is to help them get assistance and that without the information no assistance is possible; the form also tells them the kinds of agencies who might have access to the information in their files when legally necessary; the form also states that the applicant must request release of information to anyone else wants to see their files.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?** Manuals are used to insure consistency
- 2) **What are the retention periods of data in this system?** One year as per the handbook and actual case files are maintained for 5 years.
- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?** Procedures are issued yearly by contractor and consistent with handbook.
- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?** No
- 5) **How does the use of this technology affect public/employee privacy?** No affect because of existing security plan controls.
- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.** No, it does not have that capability.
- 7) **What kinds of information are collected as a function of the monitoring of individuals?** No monitoring except use of system by IT security manager.
- 8) **What controls will be used to prevent unauthorized monitoring?** Routine security measures are in place.
- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.** Social Services BIA#8, DOI sec 383 DM 1.4 F., 3.6 and 4.4C and DOI regs at 45 CFR 2.48, 2.51, 2.52, 2.56 and 2.57-2.77, Privacy Act System of Records is Interior/BIA-8.
- 10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.** No revision is occurring

F. ACCESS TO DATA:

- 1) **Who will have access to the data in the system?** Users and contractors
- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?** The handbook describes access to data by user.

- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.** The access is restricted.
- 4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials).** The handbook describes controls and there is IT security training and background checks; e.g. IT security training, background checks.
- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? (If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?)** Contractors are involved with maintenance of the system and there is no design and development.
- 6) **Do other systems share data or have access to the data in the system? (If yes, explain.)** No.
- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** No interface.
- 8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?** There are no other agencies sharing info
- 9) **How will the data be used by the other agency?** Not applicable
- 10) **Who is responsible for assuring proper use of the data?**
The regional and agency BIA and Social Service staff.

See Attached Approval Page

The Following Officials Have Approved this Document

1.) Business Owner

Jerry A. Ricketts (Signature) 8/29/07 (Date)
Name: Jerry Gidner
FOR Title: Deputy Director of Indian Services

2.) System Owner

Sanjeev Bhagowalia (Signature) 2-13-2008 (Date)
Name: Sanjeev Bhagowalia
Title: Deputy Assistant Secretary-Indian Affairs/Management
Chief Information Officer
Assistant Secretary-Indian Affairs

3.) System Manager

Gil Wake (Signature) 9/7/2007 (Date)
Name: Gil Wake
Title: Director, Office of Information Operations
Office of the Chief Information Officer

4.) IT Security Manager

Joan Tyler (Signature) 8/29/07 (Date)
Name: Joan Tyler
Title: Director, Office of Information Security and Privacy
Office of the Chief Information Officer.

5.) Privacy Act Officer

Bob Harnage (Signature) 8/22/07 (Date)
Name: Bob Harnage
Title: Director, Office of Information Policy
Office of the Chief Information Officer

6.) Reviewing Official

Sanjeev Bhagowalia (Signature) 2-13-2008 (Date)
SANJEEV BHAGOWALIA Name: Sanjeev Bhagowalia
Title: Deputy Assistant Secretary-Indian Affairs/Management
Chief Information Officer
Assistant Secretary-Indian Affairs

provided to CIO 2-12-08
CIO Signet 2-13-08 8