DEPARTMENTAL ADMINISTRATION (DA)
General Support System (GSS)

USDA

PRIVACY IMPACT ASSESSMENT (PIA)
Version 3 0

July, 2008

USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: <u>DA General Support System (GSS)</u>
Description of Program/Project:

<u>The Departmental Administration General Support System (DA GSS) provides the infrastructure to support all the Staff Offices of Departmental Administration and the headquarters staff of the Office of the Chief Financial Officer (OCFO). DA GSS services include communications, servers, email, dial up, Internet/Intranet access, and access to the National Finance Center (NFC) in New Orleans, LA and the National Information Technology Center (NITC) in Kansas City, MO.</u>

DATA IN THE SYSTEM

1 Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	The system is a GSS designed to transport information and provide file storage. It does not process information. The customers of the GSS are predominately USDA employees and contractors who use the system for administrative purposes.
2a. What are the sources of the information in the system?	Primarily information passed between DA offices, with NFC and NITC, and to other USDA offices in and outside of the Washington, DC area.
2b. What USDA files and databases are used? What is the source agency?	Departmental Administration files and databases such as personnel, finance, and procurement.
2c. What Federal Agencies are providing data for use in the system?	Primarily internal USDA Headquarters information
2d What State and Local Agencies are providing data for use in the system?	None; primarily internal information.
2e. From what other third party sources will data be collected?	Bidders, contractors.
2f. What information will be collected from the customer/employee?	Bids, contract information from vendors; employee personal data; time and attendance, and expense data from employees

3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Review by DA office responsible for data
3b. How will data be checked for completeness?	Review by DA office responsible for data

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Users, managers, system administrators
2 How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Access permissions are required; passwords are issued. Access procedures are documented.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	Access control specifies file permissions for each user.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	Rules of behavior.
5a. Do other systems share data or have access to data in this system? If yes, explain.	Information sent to NFC and NITC; reports received from NFC and NITC.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	DA network transports data and provides file storage. Data owners are responsible for proper use of data.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	No data sharing with other agencies. Data are solely used internally.
6b. How will the data be used by the agency?	GSS supports major administrative functions of the agency.
6c. Who is responsible for assuring proper use of the data?	Data owners are responsible for proper use of data.

For Official Use Only

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 System is designed to transports and provides data storage.
2a Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No. The system is used as a storage area, and no information gathering process is conducted.
2b. Will the new data be placed in the individual's record (customer or employee)?	Yes, data will be placed in individuals Official Personal Folder (OPF)
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	Yes, there is a customer number, which indentifies an employee.
2d. How will the new data be verified for relevance and accuracy?	They are checked via hardcopy. Data owners are responsible for verification and accuracy of data.
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	There is IT security policy in place, which requires user login and password in order to access the data.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	In order to access the data, each individual must fill out a request form, signed by her/his supervisor, justifying the request for access, once approved, a new username and password is created for that individual with audit trail capability.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Data are retrieved by a personal identifier like customer number.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	None of the customer's due process rights are affected by the system. None of the mentioned effects on the left column applies. The data is used to proved better customer service to employees.

4c. How are the effects to be mitigated?	The customer number is changed from SSN, in order to mitigate risk.

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	The system is shared by all employees and everyone has the same privilege on the system.
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?	They are accessed from different sites, but all access the same system.
2b. Explain any possibility of disparate treatment of individuals or groups	There is none. All have the same privilege on the system.
2c. What are the retention periods of data in this system?	It is deleted once an employee leaves DA.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Data are deleted and purged. Disk drive is destroyed / shredded by outside source.
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?	Data owners are responsible for proper use and accuracy of the data. Annual check is conducted to ensure accuracy.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No. The technology used has been around for a while.
3b. How does the use of this technology affect customer/employee privacy?	Employees privacy's risk is minimal since a proven technology is being used.
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	The system has data containing individuals location and Identity but not monitoring.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	The system applies to individuals not groups.

For Official Use Only

4c What controls will be used to prevent unauthorized monitoring?	System access is restricted and servers are located in a secure environment with control access in place.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	System operates under one SOR, OP-1
5b If the system is being modified, will the SOR require amendment or revision? Explain.	No modification needed. OP-1 is a general SOR that covers wide area.

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Department of Administration (DA) General Support System (GSS)

_____

(System Name)

This document has been completed in accordance with the requirements of the EGovernment 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.

_____   7.10.2008
System Manager/Owner   Date
OR Project Representative
OR Program/Office Head.

_____   7-10-2008
Agency's Chief FOIA officer   Date
OR Senior Official for Privacy
OR Designated privacy person

_____   7-10-2008
Agency OCIO   Date