CHAPTER 3, PART 2
PRIVACY IMPACT ASSESSMENT

1 BACKGROUND

The USDA is responsible for ensuring the privacy, confidentiality, integrity, and availability of customer and employee information. The USDA recognizes that its customers and employees have some reasonable expectation of privacy about themselves. This includes an expectation that USDA will protect personal, financial, and employment information from unauthorized disclosure. 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. Customer and employee information is protected by the following:

a Privacy Act of 1974, as Amended (5 USC 552a);
b Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g–3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems;
c OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with air information practices and security requirements for operating information systems;
d Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy; and
e The E-Government Act of 2002, 44 U.S.C. 3531 et seq.

Improvements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. This ability has raised concerns about the impact of large computerized information systems on the privacy of individual subjects of data. Public concerns about highly integrated information systems that the government operates make it imperative to commit to a positive and aggressive approach to protecting individual privacy. The Office of the Chief Information Officer (OCIO) implements the Privacy Impact Assessment (PIA), required in the E-Government Act of 2002, section 208, in order to ensure that the systems USDA develops protect individual privacy.

The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

The PIA is a process used to evaluate the impact that information systems have on an individual. The PIA process is designed to guide agency system developers and operators in assessing privacy through the early stages of development. Privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Cyber Security (CS) Privacy Officer are also parts of this process.

2 POLICY

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.

New systems, systems under development, or systems undergoing major modifications are required to complete a PIA. The CS Privacy Policy Officer may request that a PIA be completed on any system that may have privacy risks. More specifically:

a New systems and systems under development or undergoing major modifications are required to complete a PIA.

b Agencies and activities must evaluate systems already in existence to determine if a PIA should be conducted. If privacy is a concern for the existing system, the CS Privacy Officer is authorized to require a PIA. However, if an agency

makes a major change or upgrade to an existing system, the agency responsible for the system must conduct a PIA. USDA will use reasonable efforts to remedy any problems uncovered by a PIA.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this policy exception as a Plan of Action & Milestone (POA&M) in their FISMA reporting until full compliance is achieved. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

a CS will provide initial training on the PIA and additional training, as necessary. This training describes the PIA process and provides details about the privacy issues and privacy questions to be answered to complete the PIA. The intended audience is the personnel responsible for implementing the protections and completing the PIA document. PIA training is available to government and contractor personnel.

b Preparing the PIA document requires that the system operator and developer answer certain privacy questions. A copy of the questions is attached at Attachment 1. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as "Not Applicable". During the development of the PIA document, the CS Privacy Officer will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.

c The completed PIA document is to be submitted by each agency to Cyber Security for review. The purpose of the review is to identify privacy risks in the system. The CS Privacy Officer will work with the system owner and system developer to develop design requirements to resolve the identified risks.

If there are privacy risks in a system that cannot be resolved with the CS Privacy Officer, the recommendations will be presented to the ACIO for Cyber Security and USDA Chief Information Officer for a final decision.

d The System Life Cycle review process will be used to validate the incorporation of the design requirements to resolve the privacy risks. Formal approval by the Designated Accrediting Authority for the system will be issued in accordance with the CS Configuration Management Guidance, CS-009 or the formal Configuration Management Plan adopted by the agency or staff office.

The Privacy Act of 1974 5 U.S.C. 552a, as Amended, forbids Federal agencies from disclosing any information contained in a PA system of records.

"No agency may disclose any record contained in a system of records...unless the release would be in accordance with one or more of the 12 exceptions". 5 U.S.C. 552 a (b)

The PIA also requires agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

e To fulfill the commitment of the USDA to protect customer and employee data, several issues must be addressed with respect to privacy:

1 The use of information must be controlled; and

2 Information may be used only for a necessary and lawful purpose.

Where PA systems of records are involved:

1 Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them;

2 Information collected for a particular purpose should not be used for another purpose without the subject's consent unless such other uses are specifically authorized or mandated by law; and

3 Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

f Given the availability of the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the USDA, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

g These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the USDA to the laws which protect customer and employee privacy rights and which provide redress for violations of those rights.

h The sources of the information in the system are an important privacy consideration if the data is gathered from sources other than customer records. Information collected from non-USDA sources should be verified for accuracy, currency and completeness, to the extent practicable. This is especially important if the information will be used to make determinations about individuals.

i Access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system operators, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties.

j If individuals using other systems are granted access to all of the data in a system, procedures need to be in place to detect and deter browsing or unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, State, or Local entities that have access to USDA data.

k System requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. The data must be relevant and necessary to accomplish the purpose of the system. The data must also be complete, accurate and timely. These terms are defined in the Privacy Act and the Definitions Section. Each agency is responsible for determining that these requirements are met. The System of Records (SOR) Notice contains information on the confidentiality and availability of data. It is important to ensure that the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

l Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. 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.

m Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory and/or USDA Records Management requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly destroyed at the end of that time.

n The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of customers and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some judicially ascertainable standard as determined by the Office of the Inspector General (OIG) of reasonableness in light of the statutory mission of the USDA and other authorized governmental users of the system.

ATTACHMENT 1
OUTLINE OF STEPS FOR COMPLETING A PIA

Step	Who	Procedure
1	System Operator, and Developer	Request and complete Privacy Impact Assessment (PIA) training.
2	Agency ISSPM	Coordinates with System Developer to resolve questions and begin survey.
3	System Operator, and Developer	Answer the Privacy Questions. (See Attachment 1).
4	System Operator, and Developer	Submit the PIA document to the CS Privacy Officer
5	CS Privacy Officer	Review the PIA document to identify privacy risks from the information provided. The CS Privacy Officer will get clarification from the developer as needed.
6	System Operator, Developer, CS Privacy Officer, and Chief Information Officer	The System Operator, Developer and the CS Privacy Officer should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached, then issues will be raised to the Chief Information Officer for resolution.
7	System Operator, and Developer	The System Operator and Developer will incorporate the agreed upon design requirements and resolve the identified risks.
8	System Operator, Developer, and CS Privacy Officer	Participate in the SLC required reviews to ensure satisfactory resolution of identified privacy risks and obtain formal approval.
9	ISSPM	Conducts compliance reviews to ensure all agency Information systems have conducted PIA reviews, as required.

ATTACHMENT 2
USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: _____
Description of Your Program/Project:

_____
_____
_____
_____
_____

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system.	
2a. What are the sources of the information in the system?	
2b. What USDA files and databases are used? What is the source agency?	
2c. What Federal Agencies are providing data for use in the system?	
2d. What State and Local Agencies are providing data for use in the system?	
2e. From what other third party sources will data be collected?	
2f. What information will be collected from the customer?	
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	
3b. How will data be checked for	

completeness?	

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	
5a. Do other systems share data or have access to data in this system? If yes, explain.	
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	
6b. How will the data be used by the agency?	
6c. Who is responsible for assuring proper use of the data?	

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?	
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	
2b. Will the new data be placed in the individual's record (customer or employee)?	
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	
2d. How will the new data be verified for relevance and accuracy?	
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	
4b. What are the potential effects on the due process rights of customers: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	
4c. How are the effects to be mitigated?	

MAINTENANCE OF ADMINISTRATIVE CONTROLS	
1a. Explain how the system and its use will ensure equitable treatment of customers.	
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?	
2b. Explain any possibility of disparate treatment of individuals or groups.	
2c. What are the retention periods of data in this system?	
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	
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?	
3a. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?	
3b. How does the use of this technology affect customer privacy?	
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	

4c. What controls will be used to prevent unauthorized monitoring?	
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name. (SORs can be viewed at www.access.GPO.gov)	
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	