

ePermits

Privacy Impact Assessment (PIA)



Animal and Plant Health Inspection Service

Protecting American Agriculture and Natural Resources

REVISION HISTORY

Version	Date	Description
1.0	7/20/04	Initial publication of PIA
1.1	7/20/05	First revision of PIA for Certification and Accreditation
1.2	12/17/07	PIA revised for System of Records Notice

Privacy Impact Assessment Authorization

Concurrence Memorandum

I have carefully assessed the Privacy Impact Assessment for the Comprehensive Electronic Permitting System.

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.



IT Project Manager



Date




Executive Sponsor



Date



Agency's Privacy Official
OR Agency OCIO



Date

CONTENTS

USDA PRIVACY IMPACT ASSESSMENT FORM	1
DATA IN THE SYSTEM	2
ACCESS TO THE DATA.....	3
ATTRIBUTES OF THE DATA.....	4
MAINTENANCE OF ADMINISTRATIVE CONTROLS	5

USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: USDA ePermits

Description of Your Program/Project: ePermits is an automated permit processing system that is completely web-based. The application includes some functionality and data that are for internal APHIS use only. ePermits supports permitting processes for three USDA/APHIS programs: Biotechnology Regulatory Services (BRS), Plant Protection and Quarantine (PPQ), and Veterinary Services (VS). ePermits provides the ability for applicants to apply for a permit, check permit status, and view permits and other responses from APHIS—all online. ePermits also provides the ability for APHIS to generate and track permits and other responses to permit applications.

ePermits completed independent certification and accreditation in April 2006.

This Privacy Impact Assessment addresses the data, uses, and functionality for ePermits.

DATA IN THE SYSTEM

<p>1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.</p>	<p>Customer – Customers enter permit application information, check the status of permit applications, and view permit responses. Customers also collaborate with the APHIS Permit Staff to verify accuracy of the permit and to ensure all requirements are met.</p> <p>Customers include importers, import brokers, and researchers. The system uses the following information about customers:</p> <ul style="list-style-type: none">• Name, address (including mailing address), telephone number (including FAX and daytime numbers), email address, and organization name and job function.• Name, quantity, country of origin and intended use of regulated articles (organisms and materials) to be imported.• Destination addresses for shipments of regulated articles, including contact name and phone number.• Planned dates and ports of entries for shipments, planned quantities of permitted articles in shipments.• For permits that require fee payments, the system uses payment amount, payment date, the payment transaction number, and either the last 4 digits of the credit card number used, the check number, or the APHIS user fee account number.• For BRS permit applications, the applicant may declare that some permit application information is Confidential Business Information (CBI), a designation allowed under Section (b)(4) of the Freedom of Information Act, which exempts from disclosure certain types of information related to trade secrets and commercial or financial information. <p>Employee – USDA/APHIS permit staff employees review permit applications, create draft permits, review draft permits, communicate with the applicant by asking clarifying questions, review similar permits issued in the past to the same applicant or for the same organisms, and issue permits and shipment labels. PPQ inspectors inspect shipment labels, review associated permits, and input inspection reports. Inspection reports contain a list of shipped organisms and country of origin information.</p> <p>The system uses the following information about employees:</p> <ul style="list-style-type: none">• Name, address (including mailing address), telephone number (including FAX and daytime numbers), email address, and organization name and job function.• For APHIS permits staff who signs permits, the system uses a digital image of the handwritten employee signature for printing on the permit. <p>Other - State regulatory agencies review permit applications, and enter comments about draft permit conditions. Agricultural Inspectors from the U.S. Customs and Border Protection use ePermits to view permits and confirm the validity of permits.</p> <p>The system uses the following information about other individuals:</p> <ul style="list-style-type: none">• Name, address (including mailing address), telephone number (including FAX and daytime numbers), email address, and organization name and job function.
---	--

2a. What are the sources of the information in the system?	Information for permit applications is input by permit applicants (importers, import brokers, and researchers). Based on the information provided by applicants, APHIS permits staff in BRS, PPQ and VS draft permit conditions/restrictions, route a copy of the permit application and draft permit conditions to one or more State regulatory officials to review and add comments. Finally, APHIS permits staff review comments from the States and issue a final permit.
2b. What USDA files and databases are used? What is the source agency?	Only APHIS files and databases are used in this system.
2c. What Federal Agencies are providing data for use in the system?	None
2d. What State and Local Agencies are providing data for use in the system?	Regulatory Officials from the State Departments of Agriculture are providing data for use in ePermits.
2e. From what other third party sources will data be collected?	Some ePermits users submit BRS application files electronically from their own private systems using published standards. All ePermits users login to ePermits through USDA eAuthentication services. Payments for permit application fees are made through Pay.gov, which is operated by the U.S. Treasury Department.
2f. What information will be collected from the customer/employee?	The information collected from the applicant typically consists of information about the permittee (name and contact information), the names of the regulated articles that require a permit, the origin and destination of the regulated articles, and the intended use of the articles. A permit application may also include a request for shipment labels if needed. A permit application may also contain confidential business information (i.e., location, or name of persons involved), or information needed to pay an application fee. A permit typically contains the information in the permit application as well as permit conditions or restrictions.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	"Not applicable. No data from sources other than USDA records will be collected and maintained in this system."
3b. How will data be checked for completeness?	Applications are checked for completeness based on requirements defined by APHIS. Some completeness checks are automated and some are manual. For example, there are required fields in the system where the permittee is required to enter data before proceeding to the next page of the application.

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Data in the system is accessible to APHIS employees consisting of: permit writers, managers, system administrators, database administrators, and PPQ inspectors. Likewise, DHS Customs and Border Protection (CBP) inspectors and state regulatory officials will also have access to the data in this system.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Role-based security and access rights are implemented to protect the confidentiality of information. Role-based security includes the use of USDA eAuthentication services, which provides user authentication. User roles are granted through web-of-trust mechanisms in place. Criteria, procedures, controls, and responsibilities regarding access are documented in the ePermits Certification and Accreditation (C&A) documentation, the ePermits Security Plan, and Standard Operating Procedures (SOP).

3. Will users have access to all data on the system or will the user's access be restricted? Explain.	Each program approves access and roles in the system. User access to data is restricted and is based on the role of the user. Applicants see only data related to their own permit applications. APHIS permits staff view only information within their department. CBI is restricted to authorized users. Select agent permit data is restricted to authorized users.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	The ePermits security plan includes management, operational, and technical controls to prevent misuse of data by system users. Security mechanisms include firewalls, system hardening, automatic session expiration, automatic password expiration, and virtual private database functionality.
5a. Do other systems share data or have access to data in this system? If yes, explain.	No other systems share data or have access to data in ePermits.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	Not applicable. This system does not interface with another system
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, or Other)?	Yes, Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP).
6b. How will the data be used by the agency?	DHS/CBP personnel will use data from the system to ensure shipments arriving in U.S. ports have import permits.
6c. Who is responsible for assuring proper use of the data?	USDA's National Information Technology Center houses the ePermits servers and implements all security procedures. The ePermits Project Manager along with APHIS Program Managers are responsible for overseeing operations and implementing all management and operational controls.

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
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No
2b. Will the new data be placed in the individual's record (customer or employee)?	Not applicable
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	No
2d. How will the new data be verified for relevance and accuracy?	Not applicable
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	Not applicable

3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	No processes are being consolidated.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Data can be retrieved using either the applicant name or the applicant organization name provided by the applicant.
4b. What are the potential effects on the due process rights of customers and employees of: <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. 	The potential effects are all positive in nature. The general public will receive information in a more timely manner and the USDA employees will be able to process information more efficiently. Because ePermits uses a web-base technology, strong security controls have been implemented. The security controls are part of the Certification and Accreditation for all systems.
4c. How are the effects to be mitigated?	The ePermits Security Plan has been approved and is used to minimize security risks.

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	The system accepts all incoming applications for permits and are treated equally. Once received, applications are assigned to a specialist for processing. These assignments are made electronically. Thus, fair and equitable treatment are afforded to all applicants and customers who are requesting permits.
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?	Not applicable. The ePermits production system is managed and operated at the USDA National Information Technology Center (NITC), located in Kansas City, Missouri.
2b. Explain any possibility of disparate treatment of individuals or groups.	"There is no opportunity for disparate treatment of individuals or groups as each application is received into the ePermits system and assigned to a specialist for processing via electronic case assignment." "
2c. What are the retention periods of data in this system?	The data retention schedule for electronic records in ePermits is 15 years, consistent with retention schedules for policy-related information.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	The ePermits Security Plan identifies the following activities: sanitization or degaussing of system peripherals such as disks that are retired or replaced during the life of the project, sanitization of disks for client systems when employees leave the agency, and sanitization or degaussing of server disks or storage media for retired or outdated systems.
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?	Permit applications and permit data are retained in the system according to approved records management schedule. APHIS Permit Staff ensures that determinations are recorded in the system, as well as the information used to make the determination. Each APHIS program office issuing permits ensures that determinations are made about whether the data is sufficiently accurate, relevant, timely, and complete enough to ensure fairness by doing periodic quality control checks.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No

3b. How does the use of this technology affect customer/employee privacy?	Not applicable
4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u> ? If yes, explain.	The system is capable of identifying and locating individuals seeking a permit. However, this system is not designed to or capable of live monitoring.
4b. Will this system provide the capability to identify, locate, and monitor <u>groups of people</u> ? If yes, explain.	Importer and user registration information will provide the ability for a user to identify individuals or businesses if contact is necessary. However, this system is not designed to or capable of identifying or monitoring "groups of people"
4c. What controls will be used to prevent unauthorized monitoring?	Not applicable. No live monitoring involved.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	The APHIS-10 Systems of Records Notice is currently in draft form and will soon be submitted for clearance and approval.
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	Not applicable