Privacy Impact Assessment

Investigation Tracking and Enforcement Management System (ITEMS)

Technology, Planning, Architecture, & E-Government

- Version: 1.5
- Date: October 04, 2011
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

Investigation Tracking and Enforcement Management System (ITEMS)

Date: October 04, 2011

Contact Point

Cynthia Lavallee
COTR / Project Manager
United States Department of Agriculture
4700 River Road, Unit 144
Riverdale, MD 20737
301-734-7765
cynthia.g.lavallee@aphis.usda.gov

Reviewing Official

Tonya Woods, Privacy Officer
Danna Mingo, Information Security Branch
United States Department of Agriculture
(301) 851-2487

Abstract

System Name:

Investigation Tracking and Enforcement Management System (ITEMS)

System Description:

IES investigates alleged violations of Federal laws and regulations related to the mission of the Agency. The ITEMS Tracking System is used in the management of the investigations from discovery through final stipulation. ITEMS is used for preparing reports for programs within the Agency, other Federal agencies, OMB, and Congress upon request. ITEMS' provides a secure Web-based interface to an Oracle database.

A Privacy Impact Assessment (PIA) is being conducted because the data from the migrated legacy system, used as historical data for ITEMS, contains the information from the public, as subjects of an investigation or as witness information that could be personally identifiable.

Overview

The ITEMS application interface supports the entry, update, submission, and tracking of cases for all APHIS programs by conducting investigations of alleged violations of Federal laws and regulations under APHIS' jurisdiction. ITEMS will also allow users to generate reports thereby enhancing the program's ability to analyze its data and respond to Agency, public, and Congressional inquiries.

IES investigators conduct investigations inputting case information into the ITEMS' system and retaining all supporting documentation about the case. At IES Headquarters, the branch chiefs assign completed investigations to appropriate *Enforcement Specialists,* as their respective workload allows, to conduct case review activities and to assign stipulations to violators when appropriate. The IES Branch Chiefs also assign the non-investigative cases to *Case Examiners* to generate warning tickets and settlement offers. IES users also check status of a case and view case information submitted by investigators.

The ITEMS system owner and the contact information:

Robert Huttenlocker
Director
Investigative and Enforcement Services
USDA/APHIS
4700 River Road, Unit 85
Riverdale, MD 20737
(301) 734-7453
Robert.J.Huttenlocker@aphis.usda.gov

The ITEMS security point of contact is:

Cynthia Lavallee
COTR / IT Project Manager

United States Department of Agriculture
4700 River Road, Unit 144
Riverdale, MD 20737
301-734-7765
cynthia.g.lavallee@aphis.usda.gov

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The system uses the following Customer information:

Our customers are either subjects of an investigation or witnesses. The Case ID is used to refer to one or more subjects and/or witnesses. ITEMS system uses the following information about a subject:

- Name, address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and address if subject is a business
- TIN and DUNS number for business and SSN, date of birth for individuals is not a mandatory field in ITEMS, however, investigators may collect this information as a way to ensure the enforcement of fines is assessed to the right individual.
- Final disposition information for the cases and for cases that are issued penalty. The system captures penalty fees assessed, required fee payments, and uses payment amount, payment date and the payment transaction number.

The system uses the following information about IES employees:

- Name, address (including mailing address), telephone number (including work, FAX and home numbers), eAuth id, email address, and organization name and job function.

1.2 What are the sources of the information in the system?

Information in this system comes primarily from USDA employees (APHIS, AMS, and FSIS) or other investigative personnel (DHS/CBP, states regulatory officials), and on-line data sources (LexisNexis). Investigation activities, investigation findings, witness statements, interviews, documents obtained from commercial database searches, and APHIS Program records are also sources of information used in the system. Information for cases generated is entered through violation referral and is based on the information documented in PPQ-518, PPQ-591 or PPQ-592 or in the

violation referral information furnished by programs when submitting a request for investigation by IES.

1.3 Why is the information being collected, used, disseminated, or maintained?

The data collected is used in the investigation of alleged APHIS violations. The information is used track the investigation from initiation through final determination to support the prosecution of cases. The information is used to inform the violator of the stipulations and fines determined by the government. The system tracks payments of stipulations and fines. The information is also used for referral of a case to OIG, Dept of Justice, IRS, external organizations, or debt collectors.

1.4 How is the information collected?

Information is collected through a variety of investigative techniques. Interviewing (subjects, co-workers, business associates, anyone perceived as having knowledge of the individual, company or anyone having knowledge of the potential violation), site visits and requests from other investigators for additional information.

1.5 How will the information be checked for accuracy?

The investigator checks the information for accuracy, by a verifying during the verbal interview and obtaining a signed affidavit that the information is correct. The staff and investigators use the IES intelligence analysis unit (who have access to multiple open source information systems, state records, and other supporting documents) to verify accuracy of information being collected.

1.6 What specific legal authorities, arrangements, and/or agreements define the collection of information?

The notification that is published in the Federal Register that explains to the public the authorities granted to APHIS, IES to collect this type of information in support of the investigative duties assigned, is detailed in the Systems of Records Notice – APHIS-1: (7 U.S.C. 7701–7772; 21 U.S.C. 101–105, 111–134, 7 U.S.C. 2131 *et seq.*; 15U.S.C. 1821 *et seq.*; 31 U.S.C. 3711–3719.)

IES directs and coordinates investigations related through APHIS' regulatory authority which is derived from Title 9 of the Code of Federal Regulations (CFR) for Animal welfare; Horse protection; Disease eradication; Interstate movement of livestock, plants, plant products, or plant pests; Veterinary biologics; and APHIS' accredited veterinarian program. Title 7 of the CFR for Biological toxins and agents; Domestic quarantines; Endangered species; Foreign quarantines; Genetically engineered organisms; Hawaii Quarantines; Honey bees; Import/Export; Noxious weeds; Plant

pests; and the Seed Act. The information collected supports the investigation and prosecution of alleged violators to these regulations.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

PII information is no longer a mandatory field on ITEMS, however if it is collected during the course of the investigation it is encrypted through Oracle Wallet Encryption Service (AES 192) which encrypts the SSN/TIN. All migrated data from the legacy IES-TS system that may still contain PII, is also encrypted through Oracle Wallet Encryption Service (AES 192) which encrypts the SSN/TIN and only eAuthenticated government employees with appropriate clearance are able to access it.

Mitigation:

i) Access to the site is through https protocol which guarantee information transmitted through the network is encrypted

ii) Access ITEMS application is restricted through an eAuthentication

iii) SSN# / TIN is stored in an encrypted format in the database.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The principle purpose of collecting data from an individual is to collect information to notify them on the final disposition of their case, and to track status of their payment plan and inform violators on the non-payment of fines and to support the prosecution of cases from initiation to closure. This includes the possible referral of a case to OIG, Dept of Justice, IRS, external organizations, or debt collectors. The data collected will also be used to manage and issue subpoenas and notifications; perform inspections, investigations, and permit-related activities; prepare permits, letters, and other documents; generate reports to evaluate quality of the case and effectiveness of the program; determine if the action requested in the case would additionally subject to other Federal or State authorities; and facilitate and account for payments.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Data Analysis and reporting is done through Cognos. No new data is produced. The reports produced reflect the data analysis used to assist IES in tracking the types of

investigations, trends in violations captured. Using the tool IES can manage investigators, analyze cases, and identify violation trends and stipulation review.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

No, the system itself does not link to commercial or public data. The investigators have separate access to LexisNexis and other publicly available database tools verify the information collected is accurate.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

SSN and TIN#'s are stored in an encrypted form. Unauthorized users cannot extract PII from the database, which is stored in a secure data center at NITC. ITEMS uses a role based ID and Password which is eAuthenticated. The data administrator tracks and audits all users accessing the system.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The data retention schedule is determined by the type of violation in accordance with APHIS records management (NARA) and IES retention guidelines. Data retention is determined by program, by type of violation, and date of closure of the investigation. PPQ has a retention period of a minimum of 5years from data of final action. Animal Care cases investigated have an indefinite period of retention from date of final action.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, the retention period is approved and is done in accordance with the NARA and the IES Retention guidelines.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Records are not purged from the system because violator history can impact future enforcement actions. Records are kept by the program in its original format and stored.

The system restricts level of access (read-only, update, etc.) based on roles and grants minimum level of privileges needed.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

IES' primary customers include APHIS' Animal Care, Biotechnology Regulatory Services, Plant Protection and Quarantine, and Veterinary Services programs Selected individuals from other APHIS program offices, like FMD are allowed to access ITEMS, for the purpose of following up on investigations that are specific to their program's mission in supporting the enforcement of APHIS regulations. These individuals may be allowed to create a violation referral to initiate a case and will be allowed to query on their case with read-only access. If OIG needs information they request information directly from IES. Congress requests the information needed through our Legislative and Public Affairs staff. We do not provide information to IRS. The Financial Management Division forwards debt/non-payment information to the IRS through the Office of Management and Budget (OMB).

4.2 How is the information transmitted or disclosed?

The information is transmitted electronically via email or database as well as through verbal communication between program officials and mailed in a secure package by a Government approved carrier. Payments are not mailed to NFC, but are sent to a lock-box (bank) located in St. Louis, MO, who in turn sends information to the APHIS Financial Management Division.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The information pertaining to investigations are only shared on a need to know basis with the appropriate program officials. Only the information necessary is shared. On all new data no PII is collected, on legacy data all PII data is encrypted or obscured so that it is not visible.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

IES' external customers include the U.S. Department of Homeland Security's Customs and Border Protection, State cooperators; Other Federal, State, and local regulatory or law enforcement agencies; Members of the general public and other individuals who make inquiries for information regarding APHIS' regulations. PII is not shared outside the Department, the Systems of Records Notice – APHIS-1 is on file detailing the authority APHIS has to collect the data, however, personally identifiable information is not shared outside USDA. These organizations request information through the Freedom of Information Act (FOIA). The information shared with the external customer deal specifically with the violation findings and determination made on specific regulations pertaining to the cases and does not include PII. The purpose of the information is to inform about violating trends and possible violations to regulations at the state and local level.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

This is not applicable because PII is not shared outside the Department. Systems of Records Notice – APHIS-1 is on file detailing the authority APHIS has to collect the data, though, personally identifiable information is not shared outside USDA.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

This is not applicable because PII is not shared outside the Department.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

This is not applicable because PII is not shared outside the Department to external customers.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. Investigators provide verbal notice to individuals prior to collecting information and a privacy statement is provided on the EAN and on the affidavit signed by the individual providing the information. It also informs the individual about IES' System of Records Notification published in the Federal Register, USDA/APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities, USDA/APHIS

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, individuals have both the opportunity and right to decline to provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes, individuals have the right to consent to particular use of information. They exercise that right by signing the affidavit which details the information collected and the reason for collecting it, and the privacy statement on the back of the affadavit.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided verbally to individuals at the time of interview. Individuals are asked to sign a privacy statement on the back of the affadavit, which mitigates the risk associated with individuals being unaware.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals cannot gain access to their information on the system. They are able to make a FOIA request or to contact IES regarding the information of their case by submitting a written request to the system manager: Director, Investigative and Enforcement Services, USDA, APHIS, 4700 River Road, Riverdale, MD 20737-1232

7.2 What are the procedures for correcting inaccurate or erroneous information?

If inaccurate or erroneous information is found it is corrected by the individual prior to signature on the affidavit. If the inaccurate or erroneous information is found on the application, there is a provision to edit/delete incorrect data. The data can only be edited by the investigator of record or the system administrator of the system. If during

an investigation inaccurate information is discovered, it can only be corrected by that investigator or the system administrator in edit mode.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified in person at the time of interview to verify and correct the information if needed. The individuals are notified of the Privacy Act and SORN information which they are required to sign. The SORN identifies the procedures for correcting information. Stating that any individual who believes, however, that he or she has been denied any right, privilege or benefit for which he or she would otherwise be eligible as a result of the maintenance of such material may request access to the material. Such requests should be addressed to the APHIS Privacy Act Officer, LPA, USDA, APHIS, 4700 River Road, Riverdale, MD 20737-1232.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Not Applicable.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Not Applicable.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

IES documented the user access the ISO 9000 Certification, which defines the criteria, procedures, controls, and responsibilities regarding user access. User access is determined by the position and function of their job, supervisory, non-supervisory, support, etc. Program access is a read-only when requested by the program. Users are required to complete eAuth application online; roles are determined by the IES Director and access is granted by the ITEMS Administrator.

The ITEMS system Administrator will perform quarterly and annual audits in compliance with the NIST Standards, AC2.1 and AU2.3. The current IES-TS users are grandfathered in as certified eAuthenticated users to ITEMS. An AD513 will be used to document all user changes as of 11/01/2011, and will be audited both quarterly and annually.

8.2 Will Department contractors have access to the system?

Yes – If approved by IES and on a limited basis Contractors may be provided access to the system to help with troubleshooting purposes and, or verify system functionality.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All APHIS employees are required to take a mandatory IT security training every year which touches on PII as well as confidential and classified information. Also all IES employees have Secret to Top Secret level clearances and are trained in the awareness of these types of systems.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

IES-TS is the legacy system which supports ITEMS has an ATO through 2012. ITEMS has completed the C&A Phase 1 documentation and is currently in the C&A Phase 2 process and should receive an ATO by Nov. 1, 2011.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All user actions like adding new data, modifying / deleting existing data is logged for auditing purposes, by the system administrator. The current IES-TS users are grandfathered in as certified eAuthenticated users to ITEMS. An AD513 will be used to document all user changes as of 11/01/2011, and will be audited both quarterly and annually by the ITEMS system administrator.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

IES Investigators are no longer required to collect or add PII data to ITEMS; it is not a mandatory field in the system. If SSN or TIN are collected, that data is encrypted or obscured so that it is not visible. PII data is not shared.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

ITEMS is a Web Based information system, hosted at NITC, for tracking analyzing and monitoring investigation information of alleged APHIS violations from discovery through final judgment.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, the technology the ITEMS system employs does not raise privacy concerns, because, as new individuals are identified and entered into the system, PII information is not required to be collected. Migrated data from the legacy system that may still contain PII, is encrypted and only eAuthenticated government employees with appropriate clearance are able to access it. PII data is not shared.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

The ITEMS System does not use or link to 3rd party websites, however the IES intelligence team uses LexisNexis and other open source websites to verify that the publically known data collected is accurate.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

No PII is requested or made available through the 3rd party website.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable- No PII is requested or made available through the 3rd party website.

10.10 Does the system use web measurement and customization technology?

No, ITEMS does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

The ITEMS system does not use web measurement and customization technology.

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites

and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable-ITEMS does not use or link to 3rd party websites.

Responsible Officials

Cynthia Lavallee
COTR / Project Manager
United States Department of Agriculture
4700 River Road, Unit 144
Riverdale, MD 20737
301-734-7765
cynthia.g.lavallee@aphis.usda.gov

United States Department of Agriculture

Approval Signature

Name: Robert Huttenlocker
Title: IES Director, System Owner
Agency: APHIS IES
United States Department of Agriculture

Name: Rajiv Sharma
Title APHIS ISSPM
United States Department of Agriculture

Title: Acting APHIS CIO
Agency
United States Department of Agriculture

Title: APHIS Privacy Officer
Agency
United States Department of Agriculture