Privacy Impact Assessment

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: May 13, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Investigation Tracking and Enforcement Management System (ITEMS)

May 13, 2020

Contact Point

Shaquita Parker
USDA MRP IT
301-851-2750

Reviewing Official

Tonya Woods
Privacy Officer
United States Department of Agriculture
301-851-2487

Abstract

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 action. 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

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 and non-investigated cases to appropriate Investigative and Compliance Specialists or *Enforcement Specialists*, as their respective workload allows, to conduct case review activities and issue penalties to alleged violators when appropriate. IES users also check status of a case and view case information submitted by investigators.

The ITEMS system owner and the contact information:

Eileen Sullivan
Director
Investigative and Enforcement Services
USDA/APHIS
4700 River Road, Unit 85
Riverdale, MD 20737
(301) 851-2787

Eileen.F.Sullivan@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, witnesses, or government officials referring an alleged violation to IES. The Case ID is used to refer to one or more subjects and/or witnesses. ITEMS system uses the following information about a subject:

• Subject of investigation including their address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and address if subject is a business, type of infraction, copies of violations reports, compliance agreements, warning notices, Office of General Counsel recommendations to the Department of Justice (DOJ), court disposition documents, complaints, consent decision documents, and decisions and orders.

• Witness names including their address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and address if subject is a business,

• Referring official names. Referring officials are often also witnesses.

• 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.

• Information regarding the investigation case disposition and status

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 regulatory enforcement 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 forms PPQ-518, PPQ-591 or PPQ-592 or in the violation referral information furnished by programs when submitting a request for investigation by IES. Court records are received from the US Department of Agriculture Office of Administrative Law Judges and any applicable state and federal court Records.

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 to track the investigation from initiation through final determination to support enforcement action, as appropriate. The information is used to inform the alleged violator or subject of the stipulations and penalties determined by the

government. The system tracks payments of stipulations and penalties. The information is also used for referral of a case to OIG, Department of Justice or Internal Revenue Service (IRS), for debt collection or treasury offset.

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 verifying during the verbal interview and/or obtaining a signed statement, when possible. The staff and investigators use the IES intelligence analysis unit (who have access to multiple open source information systems (such as Google), state records, and other supporting documents) to verify accuracy of information being collected, in addition to other sources of evidence collected during the investigation.

1.6 What specific legal authorities, arrangements, and/or agreements defined 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.). The records in this system are used to issue invoices and collect funds due to the Government in compliance with the Debt Collection Act of 1982, Pub.L. 97-365, 96 Stat. 1749, as amended by Pub.L. 98-167, 97 Stat. 1104, and the Debt Collection Improvement Act of 1996, Pub.L. 104-134, 110 Stat. 1321; and case management information in this system is used to monitor compliance with the Government Performance and Results Act of 1996.

IES directs and coordinates investigations for laws APHIS enforces:

- Plant Protection Act
- Animal Health Protection Act
- Virus Serum Toxin Act
- Commercial Transportation of Equines to Slaughter Act
- Animal Welfare Act
- Horse Protection Act
- Agricultural Bioterrorism Protection Act
- Honey Bee Act
- Federal Seed Act

- Lacey Act import declaration requirements

Regulatory authority is derived from Titles 7 and 9 of the Code of Federal Regulations (CFR) involving Animal welfare; Horse protection; Disease eradication; Interstate movement of livestock, plants, plant products, or plant pests; Veterinary biologics; APHIS' accredited veterinarian program; 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 enforcement of 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.

SSN/TIN information is no longer a mandatory field in 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 SSN/TIN, 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.

iv) ITEMS maintains database shadow tables to keep track of users making updates to critical data information

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 is to maintain a record of APHIS investigations. This includes notifying the investigation subject(s) of the final disposition of their case, to track debt collection and to support the prosecution of cases from initiation to closure. This includes the possible referral of a case to OIG, Department 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 a reporting tool called IBM Cognos. IBM Cognos produces reports that reflect the data analysis used to assist IES in tracking the types of investigations, trends in violations captured. Using this tool, IES is able to manage workload, analyze cases, and identify violation trends, and track the status of penalty payments.

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

The investigators use LexisNexis, LexisNexis Banko, Accurint, Accurint LE Plus, Treasury Enforcement Communication System, Automated Targeting System, Emergency Action Notification System, and other publicly available tools like Public Access to Electronic Records (PACER), and other internal systems that include ePermits, SITC National Information, Communication, and Activity System (SNICAS) to verify if the information collected is accurate. In addition, they use other websites such as Secretary of State websites, Google Maps/Google Earth, eBay, SAFERSYS-USDOT and Spokeo.

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.

SSN/TIN information is no longer a mandatory field in 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 SSN/TIN, 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.

iv) ITEMS contains shadow table that tracks all people who have access to ITEMS and any changes that are made and what changes were made to critical data information.

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?

Information is kept indefinitely pending NARA approval of the records retention schedule.

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

Information is kept indefinitely pending NARA approval of the records retention schedule.

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

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

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 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. Information is shared with NFC for receipt of violation payments. Documents and information stored in ITEMS may be shared with the USDA Office of the Administrative Law Judges and with the USDA Office of the General Counsel. IES investigations are used by APHIS to form the factual basis for administrative enforcement actions, and as such IES often refers its investigations to the USDA Office of the General Counsel. The USDA Office of the General Counsel provides legal advice to APHIS and is responsible for filing and litigating administrative enforcement actions on behalf of APHIS. Such administrative enforcement actions are filed with the USDA Office of the Administrative Law Judges. IES shares information with the USDA Office of the General Counsel and the USDA Office of Administrative Law Judges as necessary to pursue and support administrative enforcement actions. This information is shared through paper reports.

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. Proper safeguards are in place and the records, both paper and electronic, are accessible only to authorized personnel. Multiple security measures are in place to prevent outsiders from entering the system. Only necessary information is shared. On all new data, SSN/TIN is not collected and on legacy data, all SSN/TIN 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?

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

1. Referral to other Federal, State, local or foreign investigative, prosecuting, or enforcement agencies, when information available indicates a violation or potential violation of law, general statute, particular program statute, rule, regulation or order, whether civil, criminal or regulatory in nature. For example, APHIS works collaboratively with the Department of Homeland Security, Customs and Border Protection, to conduct inspections and pursue enforcement actions for violations of APHIS-administered statutes, and accordingly shares information with DHS-CBP electronically in order to facilitate such enforcement. APHIS also works collaboratively with state and local agencies, and upon request, will share information with them that may relate to a potential violation of law, in accordance with the parameters outlined above.

2. Disclosure to the DOJ for use in litigation when: (a) The Agency, or any component thereof; or (b) any employee of the Agency or his or her official capacity where the Department of Justice has agreed to represent the employee; or (c) the United States Government, is a party to litigation or has an interest in such litigation; and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the records were collected.

3. Disclosure to a court or adjudicative body in a proceeding when: (a) The Agency or any component thereof; or (b) any employee of the Agency in his or her official capacity; or (c) any employee of the Agency in his or her individual capacity where the Agency has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the Agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the Agency to be for a purpose that is compatible with the purpose for which the Agency collected the records.

4. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

5. Information contained in this system of records may be disclosed to a debt collection agency when USDA determines such referral is appropriate for collecting the debtor's account as provided for in US Government contracts with collection agencies executed pursuant to 31 U.S.C. 3718.

6. Where prior collection efforts have failed, the USDA will refer to the Department of the Treasury information from this system of records concerning past due legally enforceable debts for offset against tax refunds that may become due the debtors for the tax year in which referral is made in accordance with IRS regulations at 26 CFR 301.6402-6T, offset of past-due Legally Enforceable Debt Against Overpayment, and under the authority contained in 31 U.S.C. 3720A.

7. Information contained in this system of records may be disclosed to a consumer reporting agency in accordance with 31 U.S.C 3711(e).

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.

Yes. Routine uses is covered under APHIS-1. Please refer to section 5.1 for list of routine uses.

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

Employees may share ITEMS information with external organizations three ways: electronically, verbally, or in paper format. Electronic sharing, such as through email, means that the transmission must follow agency email policies. For paper format, employees must use secure envelopes when sharing information to safeguard the confidentiality of data and to prohibit unauthorized access. If employees communicate information verbally, then standard PII (Personal Identifiable Information) protocols must be used, including transmission only on a need to know basis.

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

The identified privacy risk was the further disclosure of information pertaining to point of contact and information of alleged violators to outside sources. To mitigate this risk, employees follow agency policies when they disclose or share information. These policies are in place to protect the data against misuses and to safeguard its confidentiality.

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 Does this system require a SORN and if so, please provide SORN name and URL.

ITEMS uses the APHIS-1 SORN,
https://www.ocio.usda.gov/sites/default/files/docs/2012/APHIS-1.txt

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

Yes. Investigators provide oral notice to individuals prior to collecting information and a privacy statement is provided on the Emergency Action Notification (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

6.3 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.

6.4 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 affidavit.

6.5 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 orally to individuals at the time of interview. Individuals are asked to sign an affidavit that contains a privacy statement, 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/Privacy Act request or to contact IES regarding their information by submitting a written request to: the system manager: Director, Investigative and Enforcement Services, USDA, APHIS, 4700 River Road, Riverdale, MD 20737-1232 also include PA contact information.

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 or by email at APHISPrivacy@usda.gov.

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 in 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 IES-TS users were

grandfathered in as certified eAuthenticated users to ITEMS. An AD513 is 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 clearance levels ranging from Secret to Top Secret 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?

ITEMS has completed C&A Phase 2 and received the Authority to Operate (ATO) on December 7, 2017.

The ATO expires on December 7, 2020.

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

All user actions like adding new data, modifying and/or 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 is 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 third party websites, however the IES intelligence team uses LexisNexis and other open source websites to verify that the publicly 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 third party website. The ITEMS System does not use or link to third party websites.

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 third party website. The ITEMS System does not use or link to third party websites

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 third party website. The ITEMS System does not use or link to third party websites

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 third party website. The ITEMS System does not use or link to third party websites

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 third party website. The ITEMS System does not use or link to third party websites

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 third party website. The ITEMS System does not use or link to third party websites

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 third party website. The ITEMS System does not use or link to third party websites

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 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 third party websites.

Responsible Officials

Eileen Sullivan, USDA APHIS IES

United States Department of Agriculture

Approval Signature

PRESTON GRIFFIN Digitally signed by PRESTON GRIFFIN Date: 2020.06.08 13:30:23 -04'00'

Preston Griffin
Acting APHIS Information System Security Program Manager
Animal and Plant Health Inspection Service
United States Department of Agriculture

KATHERINE VAGNONI Digitally signed by KATHERINE VAGNONI Date: 2020.06.15 10:52:44 -04'00'

Tonya Woods
APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture

EILEEN SULLIVAN Digitally signed by EILEEN SULLIVAN Date: 2020.06.02 07:50:08 -04'00'

Eileen Sullivan
System Owner – APHIS ITEMS
Animal and Plant Health Inspection Service
United States Department of Agriculture