USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Investigation Tracking and Enforcement Management System (ITEMS)
Program Office	IES
Mission Area	APHIS MRP
CSAM Number	1907
Date Submitted for Review	November 3, 2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Angela Cole	202-465-6265
Information System Security Manager	Erica Alston	301-851-3106
System/Program Managers	Andrea McNally	202-799-7026

Abstract

The Investigative and Enforcement Service (IES) is a program office within the USDA Animal and Plant Health Inspection Service (APHIS) that investigates alleged violations of APHIS-administered law. The Investigation Tracking and Enforcement Management System (ITEMS) is a case management system used to track and manage investigations conducted by IES. All information collected during the investigation is managed in ITEMS. ITEMS collects the personally identifiable information (PII) of alleged violators of APHIS-administered law, including their name, address, email address, phone number, signature and third-party data source numbers, such as Data Universal Numbering System (DUNS). The system also collects criminal background check information, which sometimes includes social security numbers (SSNs) and dates of birth. Additionally, the system collects the name, phone number and email address of referring officials and witnesses related to the case.

Overview

APHIS protects the health of U.S. agriculture and natural resources against invasive pests and diseases, regulates genetically engineered crops, administers the Animal Welfare Act, and helps people and wildlife coexist. APHIS also certifies the health of U.S. agricultural exports and resolves phytosanitary and sanitary issues to open, expand, and maintain markets for U.S plant and animal products. The Investigative and Enforcement Service (IES) is a program office within APHIS responsible for enforcing regulations to protect the health and care of animals, plants, and agricultural industry.

IES provides investigative, enforcement, and regulatory support services to four APHIS programs. These programs include:

- Animal Care (AC) establishes standards of humane care and treatment of animals through inspections and educational efforts.
- Biotechnology Regulatory Services (BRS) protects plant health by implementing APHIS regulations for certain organisms developed using genetic engineering that may pose a risk to plant health.
- Plant Protection and Quarantine (PPQ) protect and improves the health, quality, and marketability of animals, animal products, and veterinary biologics in the U.S. by preventing, controlling, and/or eliminating animal diseases, and monitoring, and promoting animal health and productivity.
- Veterinary Services (VS) protects and improves the health, quality, and marketability of animals, animal products, and veterinary biologics.

IES also provides these services for agricultural quarantine inspection (AQI) activities carried out by the Department of Homeland Security (DHS), Customs and Border Protection (CBP).

IES' work is divided between two groups: (1) Investigations, and (2) Enforcement. Field investigators conduct investigations and produce reports of investigation (ROIs), and headquarters enforcement staff members review completed ROIs and exhibits for evidentiary sufficiency. When the information

and evidence gathered during an investigation supports the finding of a violation, APHIS may pursue enforcement action against that person or entity.

A traditional transaction begins with a referral of violation of APHIS-administered laws. Potential violations may be discovered via routine checks of licensed animal or agricultural vendors or via notification from the public (i.e., concerned individual and/or special interest group). When APHIS personnel discover a potential violation of an APHIS-administered law, they may request a formal investigation by IES – also known as a referral. A case may involve one or more individuals and/or businesses.

Examples of violations may include:

- Inappropriate handling of animals
- Importation of prohibited fruit by a food manufacturer
- Failing to accurately complete Interstate Certificates of Veterinary Inspection that were used to transport equines across state lines
- Transporting a horse that exhibited clinical signs of illness across state lines without the proper documentation
- Delinquent payments

EIS issues an Emergency Action Notification (EAN) to inform the owner, agent, or importer of a violation. In certain instances, DHS CBP may make the initial contact and provide quarantine instructions.

APHIS has several available options to resolve a case in which the evidence substantiates that an alleged violation has occurred. Enforcement actions may include an official warning, a voluntary settlement agreement, a referral to USDA's Office of the General Counsel (OGC) to institute an administrative proceeding or, in cases involving the most serious violations, a referral to the U.S. Department of Justice (DOJ) for civil or criminal action.

ITEMS is the case management system used to track and manage these investigations by IES, and supports the entry, update, submission, and tracking of cases for all APHIS programs during investigations of alleged violations of Federal laws and regulations under APHIS' jurisdiction.

When a new case is created in ITEMS, a system-generated number is assigned to a case, and all associated evidence is managed under the case. IES investigators enter case information and retain all supporting documentation about the case in ITEMS.

Information related to cases in ITEMS is received internally from the USDA Office of the General Counsel (OGC) and USDA Office of Administrative Law Judges (OALJ). Information is shared externally with the Department of Homeland Security Customs and Border Protection (CBP) and the DOJ. Information is authorized to be collected in ITEMs under the various laws and regulations that APHIS enforces.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

What legal authorities and/or agreements permit the collection of information by the project or system?

IES directs and coordinates investigations into laws and regulations that APHIS enforces. This includes running and saving criminal background checks, which sometimes include social security numbers, to understand an alleged violator's criminal and financial history. These laws consist of:

- 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
- Honeybee Act
- Federal Seed Act
- Lacey Act import declaration requirements

The regulatory authority under which IES directs and coordinates investigations, including running the background checks, are 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.

In addition to allowing for the investigation and enforcement of the above laws and regulations, 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.

Has Authorization and Accreditation (A&A) been completed for the system?

ITEMS received the Authority to Operate (ATO) on September 20, 2023. The ATO expires on September 4, 2026. Azure Government maintains a FedRAMP High Provisional ATO issued by the Joint Authorization Board. This system is authorized to store PII data with authorized levels of security controls.

What System of Records Notice(s) (SORN(s)) apply to the information?

The information collected, maintain, stored, and shared by ITEMS is covered under USDA/APHIS-1 Investigative and Enforcement Records Regarding Regulatory Activities SORN, November 16, 2001(66 FR 57698).

Is the collection of information covered by the Paperwork Reduction Act?

Yes, the APHIS Form 7162 (affidavits) is used to collect information.

Section 2: Characterization of the Information

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

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

Identifying Numbers

- Social Security number

Biographical Information

- Name (Including Nicknames)
- Business Mailing Address (sole proprietor)
- Date of Birth (MM/DD/YY)
- Business Phone or Fax Number (sole proprietor)
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Personal Email Address
- Business Email Address

Distinguishing Features

- Signatures

Specific Information/File Types

- Law Enforcement Information
- Civil/Criminal History Information/Police Record

What are the sources of the information in the system/program?

Most of the PII in the system (names, addresses, email addresses, phone numbers) comes from witnesses and individuals who refer cases to IES.

Additional background documents that can include criminal history, social security numbers, dates of birth and DUNS numbers come from commercial data sources (Lexis Nexis, Dun and Bradstreet, Clear and Transunion).

How is the information collected?

Cases can be referred to IES by an individual through an online intake form or via email to a dedicated IES inbox. If a case is received via email, IES team members manually enter the information into ITEMS. IES team members may follow up with additional interviews, speaking with individuals who are familiar with the alleged violator, including co-workers and business associates. Any additional information is manually entered into ITEMS by the IES investigator.

Background checks are conducted by IES team members who run individual criminal history and background reports directly from Lexis Nexis, Dun and Bradstreet, Clear and Transunion and manually upload copies of the reports into ITEMS.

Individuals providing affidavits fill out the Affidavit form (Form 7162) and email it to the IES team.

Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Background investigative materials are gathered from online commercial data sources (LexisNexis, Dun & Bradstreet, Clear and Transunion) in order to provide context about individuals or businesses under investigation, including their financial and criminal history. This information may include the contact information of individuals, any legal cases they have been involved in, their DUNS number, dates of birth and social security number.

How will the information be checked for accuracy? How often will it be checked?

IES investigators are trained to check the information for accuracy at the time of collection, by verifying during the verbal interview and/or obtaining a signed statement, when possible. The IES intelligence analysis unit also verifies the accuracy of information being collected by comparing it to other sources of evidence collected during the investigation.

Does the system/program use third-party websites?

No

What is the purpose of the use of third-party websites?

Not Applicable

What PII will be made available to the agency though the use of third-party websites?

Not Applicable

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Mitigation: IES team members are trained to cross-check information from multiple sources to ensure that it is accurate. For example, the PII of a violator will be checked with other records, including witness statements and data from commercial sources (Lexis Nexis, Dun and Bradstreet, Clear and Transunion).

Section 3: Uses of the Information

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

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The PII collected is used in the investigation of alleged APHIS violations. It provides the ability to track the investigation from initiation through final determination to support enforcement actions, as appropriate. The information is used to understand who the alleged violator is, to be able to interview them and other witnesses, and to inform the alleged violator or subject of the stipulations and penalties determined by the government. The background checks and criminal history are used to understand if the alleged violator has had any past violations that could potentially provide context for the current investigation and to understand if the alleged violator could potentially be a threat to the safety of the IES investigator who may be interviewing them in person.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: There is a risk that information will be used outside of its intended purposes.

Mitigation: Information in the system is only used to manage investigation and enforcement actions for APHIS laws and regulations and as outlined in SORN. Access to the system is limited to individuals that are working on the investigation cases and who require it for their job responsibilities. User roles are determined by the IES Director, and access is granted by the ITEMS system administrator. Quarterly and annual audits are performed by the ITEMS APHIS System Administrator to confirm that access is still required.

Section 4: Notice

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

How does the project/program/system provide notice to individuals prior to collection?

APHIS provides notice to individuals through a Privacy Act statement, this PIA, and the SORN. Individuals who are subject to an investigation by IES are informed of the investigation orally or by written notice.

What options are available for individuals to consent, decline, or opt out of the project?

Individuals who are subject to investigations for allegedly violating APHIS-administered laws do not have the right to opt out of investigations. Witnesses and other individuals relevant to the case who are providing affidavits voluntarily provide their information.

Privacy Impact Analysis: Related to notice.

Privacy Risk: There is a privacy risk of data subjects being unaware of how IES uses the information that is collected in ITEMS.

Mitigation: APHIS provides notice to individuals through a Privacy Act statement, this PIA, and the associated SORN.

Section 5: Data Retention

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

What information is retained and for how long?

All information in the system is retained for seven years after the closure of the case.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes (records schedule NC1-310-77-2).

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: There is a risk that records will be retained for longer than necessary.

Mitigation: The ITEMS seven-year retention period allows a reasonable amount of time to review past cases when needed, such as in cases of new information or new investigations of past offenders, while deleting records beyond that. After seven years, records in ITEMS are deleted following the NARA-approved record retention schedule.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

The USDA Office of the General Counsel (OGC) and Office of Administrative Law Judges (OALJ) share copies of case summaries with IES. These case summaries contain the names of the alleged violators and high-level information about the cases. They provide context for IES investigations in order to understand the facts and background of the cases. The information is emailed to IES. An IES team member then manually uploads a copy of the case to ITEMS.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: There is a risk of unauthorized access to the case files that are received from OGC and OALJ.

Mitigation: The IES team has a dedicated email address to receive the case files, which keeps it separate from other inboxes, thereby reducing the risk of unintentional exposure or misuse. Access to the dedicated inbox is limited to only individuals who need to access the information and to add it to ITEMS.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Third party commercial data sources:

- Background check reports are run using third party commercial sources (LexisNexis, Dun & Bradstreet, Clear and Transunion) in order to provide context about individuals or businesses under investigation, including their financial and criminal history. This information may include the contact information of individuals, any legal cases they have been involved in, their DUNS number, dates of birth and sometimes their social security number (if included in the report). The background check reports are manually downloaded from these services and then uploaded into ITEMS.
- DHS CBP: APHIS may manually share case information, which includes the PII of alleged violators and witnesses, with CBP to facilitate investigative and enforcement efforts related to specific alleged violators. The data would be extracted from ITEMS APHIS and shared by encrypted email.
- U.S. DOJ: APHIS may manually share case information, which includes the PII of alleged violators and witnesses, with the DOJ to facilitate investigative and enforcement efforts related to specific alleged violators. The data would be extracted from ITEMS APHIS and shared by encrypted email.

Additionally, information may occasionally be shared externally in exceptional cases, such as data breaches and congressional inquiries. A full list of these scenarios is listed in the SORN. Any data sharing in these scenarios would be done so in a secure manner, such as through the use of encrypted email.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: There is a risk of misuse of, unauthorized access to, or unauthorized disclosure of information while sharing externally.

Mitigation: To mitigate this risk, employees follow agency policies when they disclose or share information. A record is kept on file of each disclosure, including the date the disclosure was made, the agency to which the information was provided, the purpose of the disclosure, and a description of the data provided. All information is emailed using encryption, which ensures that it remains unreadable to unauthorized users.

Section 7: Redress

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

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

APHIS has exempted some IES records from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(k)(2). Individual access to these records may impair investigations and alert subjects of investigations that their activities are being scrutinized and thus allow them time to take measures to prevent detection of illegal action to escape prosecution. However, APHIS still accepts requests to access information in the system. APHIS reviews all access requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of APHIS, and in accordance with procedures and points of contact published in the applicable SORNs.

Individuals can seek access to his or her APHIS records by filing a Privacy Act or Freedom of Information (FOIA) request for IES consideration. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person may file a FOIA request. USDA offers several avenues to request access to their records. Individuals may file a Privacy Act or FOIA request to view their record by submitting a FOIA request online through USDA's Public Access Link (PAL), or through mail, email or fax:

USDA – Animal and Plant Health Inspection Service
APHIS Privacy Act Officer,
Legislative and Public Affairs, APHIS,
5601 Sunnyside Ave. Ap-740, Beltsville, MD 20705.
Fax: 301-734-5941
Email: APHISPrivacy@usda.gov

Further information about Privacy Act and FOIA requests for APHIS records is available at APHIS Freedom of Information Act home page.

What are the procedures for correcting inaccurate or erroneous information?

An individual may request to correct his or her records in ITEMS by filing a Privacy Act request. The request should clearly state the information that is being contested, the reasons for contesting it, and the proposed amendment to the information. Additionally, IES allows the individual to correct information at any time during the investigation. If inaccurate or erroneous information is found, it is corrected by the individual prior to signature on the affidavit. If 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.

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

The USDA/APHIS - 1 Investigative and Enforcement Records Regarding Regulatory Activities SORN provides individuals with guidance regarding the procedures for correcting information. This PIA also provides similar notice. Individuals are notified in person at the time of interview by IES personnel procedures on how verify and correct the information if needed. Additionally, APHIS notifies individuals of the Privacy Act and FOIA procedures on the APHIS website.

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

APHIS offers individuals formal redress opportunities as outlined in the questions above.

Privacy Impact Analysis: Related to redress.

Privacy Risk: There is a risk that individuals will not be able to access or update their information or be aware of how to do so.

Mitigation: APHIS provides individuals with access, amendment, or correction to their records through multiple avenues, including submitting Privacy Act requests and direct contact with the APHIS investigator. Individuals are informed of these rights via the SORN, this PIA, the APHIS Privacy Act website and verbal contact with the investigator. The redress opportunities requested may, however, be exempt from disclosure under the Privacy Act because IES records, with respect to an individual, may sometimes contain investigatory sensitive information. The release of sensitive investigator information could possibly compromise ongoing investigatory and enforcement action.

Section 8: Auditing and Accountability

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

How is the information in the system/project/program secured?

All information is secured through appropriate technical controls to prevent the misuse of data. User access to ITEMS is limited to personnel who need the information to perform their job functions. Only users with proper permissions, roles, and security attributes are authorized to access the system. Each user is obligated to sign and adhere to a user access agreement, which outlines the appropriate rules of behavior tailored for ITEMS. The system administrator is responsible for granting the appropriate level of access. Finally, all IES employees are trained in the use of information in accordance with IES policies, procedures, regulations, and guidance.

ITEMS is hosted on a federal government Azure platform that includes enhanced encryption and data monitoring and can only be accessed through the USDA local area network and virtual private network. This reduces the risk of the information being compromised and ensures that information in the system remains unreadable to unauthorized users.

All user actions, such as adding new data, modifying data and/or deleting existing data, are logged for auditing purposes by the system administrator. This allows the system administrator to understand who made changes and when in case information is mishandled.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

User access is determined by the position and function of the individual's job, including separate roles for supervisors, non-supervisors, support staff, etc. Users are required to complete an eAuth application online; roles are determined by the IES Director, and access is granted by the ITEMS System Administrator. The ITEMS System Administrator performs quarterly and annual audits of users to confirm that access is still required. If access is no longer required, it is removed. The process for granting access to the system is documented.

How does the program review and approve information sharing requirements?

If a request to share information in the system were to be received, the legality of the request would be evaluated with legal counsel. Ultimate approval of the request would come from the IES director, if the request were to be necessary and legally valid.

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

All APHIS employees are required to take a mandatory Information Security Awareness Training every year which covers 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 and the data they contain.