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."
3/12/2025	1.2	FOIAXpress EO-14168 Updates

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	eCASE – FOIAXpress/PAL
Program Office	OGC
Mission Area	DAITO
CSAM Number	2318
Date Submitted for Review	3/17/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Corey Medina	Corey.medina@usda.gov	202- 573-2810
Information System Security Manager	Lisa McFerson	Lisa.mcferson@usda.gov	202-720-8599
System/Program Managers	Alexis Graves	Alexis.graves@usda.gov	202-690-3318

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

This PIA is for the eCASE-FOIAXpress/PAL application. This is a SaaS application that is used to manage the entire lifecycle of Freedom of Information Act (FOIA) and Privacy Act (PA) requests from initial request to the final delivery of records. The FOIA and PA process allows individuals to request access to federal agency records. The application gathers PII information to both communicate with and deliver responsive records to individuals who submit FOIA and PA requests to USDA.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The General Counsel’s Office of Information Affairs (OIA) is the component responsible for the USDA’s Departmental FOIA program. USDA’s General Counsel serves as USDA Chief FOIA Officer (CFO) and provides oversight on USDA’s administration of the FOIA.

To assist with oversight, USDA utilizes FOIAXpress and PAL to manage the entire lifecycle of FOIA and PA requests from initial request to the final delivery of records. The system includes request tracking, correspondence, fee and invoice management, record review, culling and redaction, and reporting. The system is hosted on a FedRAMP approved cloud infrastructure at a single site. It stores information for individuals who have made FOIA or PA requests to USDA agencies. Individual information is used to both communicate with and deliver responsive records to FOIA/PA requesters. FOIAXpress and PAL applications do not share information with external applications. USDA’s collection and maintenance of information in FOIAXpress is authorized by the FOIA, 5 U.S.C. § 552, as amended, and the Privacy Act of 1974, 5 U.S.C. § 552a. FOIA records are also retained in accordance with National Archives and Records Administration’s (NARA) General Records Schedule (GRS) 14.

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.

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

USDA's collection and maintenance of information in FOIAXpress and PAL is authorized by the FOIA, 5 U.S.C. § 552, as amended, and the Privacy Act of 1974, 5 U.S.C. § 552a.

FOIA records are retained in accordance with NARA's GRS 14.

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

ATO Date: 9/30/2024

ATO Expires: 9/30/2027

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

Freedom of Information Act (FOIA) and Privacy Act (PA) Requests and Administrative Appeals Files. USDA/ OCIO–03

https://www.gpo.gov/fdsys/pkg/FR-2018-04-03/pdf/2018-06759.pdf

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

No, currently the Paperwork Reduction Act does not cover FOIAXpress/PAL. In the near future, the public will be able to submit Privacy Act requests electronically using the PAL system. The collection form is assigned OMB Control # 0503-0030

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.

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

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☐ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☒ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☐ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☐ Taxpayer Identification number	☐ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☐ Personal Bank Account number	☐ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☒ Personal Mobile number

☐ Health Plan Beneficiary number

☒ Business Mobile number (sole proprietor)

☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)

☐ Ethnicity

☐ City or County of Birth

☐ Citizenship

☒ Home Address

☐ Spouse Information

☐ Race

☒ Personal Email Address

☐ Employment Information

☐ Education Information

☐ Professional/Personal References

☒ Business Mailing Address (sole proprietor)

☒ Business Phone or Fax Number (sole proprietor)

☒ Group Organization/Membership

☐ Immigration Status

☒ ZIP Code

☐ Children Information

☐ Nationality

☒ Business Email Address

☒ Alias (Username/Screenname)

☐ Resume or Curriculum Vitae

☐ Date of Birth (MM/DD/YY)

☐ Country of Birth

☐ Religion/Religious Preference

☒ Home Phone or Fax Number

☐ Marital Status

☐ Military Service Information

☐ Mother’s Maiden Name

☐ Global Positioning System (GPS)/Location Data

☐ Personal Financial Information (Including loan information)

☐ Business Financial Information (Including loan information)

Biometrics

☐ Fingerprints

☐ Retina/Iris Scans

☐ Hair Color

☐ Video Recording

☐ DNA Sample or Profile

Distinguishing Features

☐ Palm Prints
☐ Dental Profile
☐ Eye Color
☐ Photos
☐ Signatures

Characteristics

☐ Vascular Scans
☐ Scars, Marks, Tattoos
☐ Height
☐ Voice/Audio Recording
☐ Weight

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)
☐ Cell Tower Records (e.g., Logs, User Location, Time)
☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information
☐ Workers' Compensation Information
☐ Mental Health Information
☐ Patient ID Number
☐ Disability Information
☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files
☐ Health Information
☒ Case Files
☐ Law Enforcement Information
☐ Academic/Professional Background Information
☐ Security Clearance/Background Check
☐ Credit History Information
☐ Civil/Criminal History Information/Police Record
☐ Taxpayer Information/Tax Return Information

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

Individuals making FOIA and PA requests provide personal contact information so that USDA analysts can reach out should they have questions about the request but most importantly, so that analysts can provide records responsive to their request(s). Generally, any person – United States citizen or not – can make a FOIA request.

2.2.1. How is the information collected?

Individuals submit their request by providing their contact information via mail, facsimile, email, and/or using PAL to create an online FOIA portal account.

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

No

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

Information entered from mail, facsimile, or email communications is verified as FOIA officers communicate with the requester. Information entered using PAL is verified for accuracy by the individual requester, who is responsible for entering, checking, and changing their information as needed to receive their desired records.

2.5. Does the system/program use third-party websites?

Not applicable

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

N/A

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

N/A

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

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

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

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.

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

The FOIA is a federal statute that provides that any person has the right to request access to federal agency records. FOIA also establishes a presumption that records in the possession of the agencies and departments of the Executive Branch of the U.S. Government are accessible to the people, except to the extent those records are protected from disclosure by any of nine exemptions contained in the law. The information collected in FOIAXpress is used to respond to requests under FOIA or the PA, to track these requests in order to maintain compliance with statutory response times, and to maintain documents responsive to these requests in compliance with legal retention and disposition schedules, including any records that are exempt from disclosure to the requester under FOIA or the PA. The information is also used to generate annual aggregate reports to the Department of Justice (DOJ) as required by FOIA.

3.2. 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.

The system automatically searches for new FOIA or PA requests for potential duplication. If duplicate records are detected, the system displays a warning message identifying the potential duplicates and allows USDA FOIA staff to either flag the new record as duplicate or ignore the warning and accept the new record as valid.

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, **leading to breaches of confidentiality and trust.**

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: By implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

> Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.
>
> Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.
>
> User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

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.

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

A Government Banner and Rules of Behavior (ROB) banner are generated to all users during sign-on. FOIA requestors submitting a FOIA via PAL can accept or decline that they are signing into a federal system, and the information collected will be used to process the FOIA request. The FOIA requestor may decline not to use the system and submit their FOIA request in hard copy.

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

Submitting FOIA requests is voluntary. Also, if a requester does not want to use PAL for submission, they can submit their request via other means such as mail, fax, or email.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: Data Retention

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

5.1. What information is retained and for how long?

USDA retains contact information for six (6) years after the last FOIA or PA request for an individual requester.

5.2. 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 are retained in accordance with National Archives and Records Administration’s General Records Schedule 14.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: There is a risk of retaining information for longer than necessary.

Mitigation: Contact information is retained in order to facilitate communication between USDA FOIA officers and requesters. Once all the requests made by a requester are closed, the requester’s contact information is purged from the system. Contact information is reviewed routinely to ensure only necessary contact information is retained (that is, only contact information associated with currently active requests are retained in the system.

Section 6: Information Sharing

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

6.1. 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?

Requester's contact information is not shared with internal organizations and/or systems.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

6.3. 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?

Requester's contact information is received and shared with any executive federal agency subject to the FOIA.

In the course of processing records responsive to FOIA and/or PA requests, it is not uncommon for agencies to locate records which either originated with another agency, or another component within their agency, or which contain information that is of interest to another agency or component. The long-standing practice in such situations is to either refer the requested record to the originating agency or component for it to process, or to consult with the other agency or component that has equity in the document to get its views on the sensitivity of the document's content prior to making a disclosure determination. Typically, agencies refer records for direct handling to another agency when the records originated with that other agency. By contrast, when records originated with the agency processing the request, but contain within them information of interest to another agency, the agency processing the request will typically consult with that other agency prior to making a release determination.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: Privacy risks associated with external sharing and disclosure include:

Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Communication of individual contact information is not possible within the system, rather, system users send contact information, usually using email, to their counterparts in another FOIA office in a different department. The purpose of this sharing is to expedite delivery of accurate and responsive records in response to a FOIA request. The sharing of this contact information is consistent with the normal use of the data described in SORN: Freedom of Information Act (FOIA) and Privacy Act (PA) Requests and Administrative Appeals Files. USDA/ OCIO–03

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.

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

Individuals gain access to their contact information using the PAL application for their account. They are able to make any necessary changes there. For individuals without a PAL account, an individual can gain access to their contact information by contacting a USDA FOIA official or by submitting a FOIA request.

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

Procedures to correct individual contact information are as described in section 7.1 above.

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

Individuals with PAL accounts see a “My Account” link which enables them to make necessary changes.

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

Individuals with PAL accounts are able to make changes to their contact information as necessary.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: **Privacy Act risks associated with redress include:**

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency’s accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Mitigation: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8: Auditing and Accountability

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

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

Access to the system and data are determined by business needs and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls are in place to ensure the correct handling of information. End users are correctly identified and authenticated according to USDA security policies for access management, authentication and identification controls. Data is encrypted both in transit and at rest. The system logs all access to requester contact information which can then be reviewed via the audit logs.

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

FOIAXpress uses a licensed user model, and Agency FOIA Officers determine which employees/contractors in their agency should have access to the application. They submit forms to the system administrator who then adds their information to the application (along with their eAuth identifier) which then lets them login if they are also logged into the USDA network. PAL users (members of the general public) access that system via a user login/password. Once logged in PAL users can see the status of request(s) they've previously submitted.

8.3. How does the program review and approve information sharing requirements?

FOIAXpress and PAL do not have information sharing requirements.

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

All users must complete annual security/privacy training in USDA's online training repository, AgLearn. Failure to complete the training results in deactivation of an individual's eAuth account, which in turn deactivates their FOIAXpress account.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 6/20/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed:TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.25 21:31:55 -04'00'
____

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:____

Alexis Graves
System Owner
OGC
U.S. Department of Agriculture

Signed:____

Corey Medina
Privacy Officer
DAITO
U.S. Department of Agriculture

Signed:____

Sullie Coleman
CISO/ACISO
DAITO
U.S. Department of Agriculture