U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risks associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Civil Rights Management System (CRMS)

Office of the Assistant Secretary for Civil Rights

Departmental Administration Information Technology Office (DAITO)

Date PIA submitted for review:

1/25/2024

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	Corey Medina	@usda.gov	202-577-8021
Information System Security Manager	Tracy Haskins	Tracy.Haskins@usda.gov	202-720-8599
System/Program Managers	Michael Dykes	Michael.Dykes@usda.gov	202-720-8106

Abstract

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

The Civil Rights Management System (CRMS) is a USDA Salesforce-based application designed to help manage, track, and report on civil rights complaints and cases. It supports USDA programs related to Title VI, Title IX, Section 504, and Limited English Proficiency by streamlining the complaint process.

CRMS allows the USDA to efficiently collect and process complaints while maintaining records of both USDA employees and the general public involved in these cases. The system captures Personally Identifiable Information (PII) such as names, roles, emails, and complaint details for employees, while complainants may provide additional details like date of birth, race, ethnicity, and sex.

A Privacy Impact Assessment (PIA) is required for CRMS because it collects sensitive personal information. This ensures the system follows privacy and security standards to protect user data while enabling the USDA to fulfill its civil rights responsibilities.

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.

CRMS collects and processes personally identifiable information (PII) from both USDA employees and the general public. USDA employees who manage complaints have accounts that include their name, role, email, and login credentials. Members of the public who file complaints may provide additional details such as name, date of birth, race, ethnicity, and sex to support their case.

CRMS Administrator staff can view all complaint records based on their access level, while complainants can only submit complaints through the public-facing portal

Section 1.0 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?

5 U.S.C. 301, 42 U.S.C. 2000d, et seq., 42 U.S.C. 3608(d); 42 U.S.C. 12101, et seq.; 20 U.S.C. 1681, et seq.; 29 U.S.C. 794; 15 U.S.C. 1691, et seq; and 7 U.S.C. 2011, et seq.

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

Yes, it expires 9/30/2024.

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

USDA/OASCR-1, Civil Rights Enterprise System (CRES) - 83 FR 65135 (December 19, 2018)

USDA/OASCR–2, Civil Rights Management System, (CRMS) – 86 FR 45952 (August 17, 2021)

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

Yes

Section 2.0 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	□	License Plate Number
□	Registration Number	□	File/Case ID Number
□	Student ID Number	□	Federal Student Aid Number
□	Passport number	□	Alien Registration Number
□	DOD ID Number	□	DOD Benefits Number
□	Employee Identification 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	□	Business Mobile Number (sole proprietor)
□	Health Plan Beneficiary Number		

Biographical Information

☒	Name (including nicknames)	☒	Sex (Female or Male)	□	Business Mailing Address (sole proprietor)
☒	Date of Birth (MM/DD/YY)	☒	Ethnicity	□	Business Phone or Fax Number (sole proprietor)
☒	Country of Birth	☒	City or County of Birth	□	Group/Organization Membership
☒	Citizenship	☒	Immigration Status	☒	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☒	Spouse Information			□	Children Information
□	Marital Status	□	Military Service Information	□	Mother's Maiden Name
☒	Race	☒	Nationality	□	Global Positioning System (GPS)/Location Data
☒	Personal e-mail address	☒	Business e-mail address	□	Personal Financial Information (including loan information)
☒	Employment Information	□	Alias (username/screenname)	□	Business Financial Information (including loan information)
□	Education Information	□	Resume or curriculum vitae	□	Professional/personal references

Biometrics/Distinguishing Features/Characteristics

□	Fingerprints	□	Palm prints	□	Vascular scans
□	Retina/Iris Scans	□	Dental Profile	□	Scars, marks, tattoos
□	Hair Color	□	Eye Color	□	Height
□	Video recording	□	Photos	□	Voice/ Audio Recording
□	DNA Sample or Profile	□	Signatures	□	Weight

Medical/Emergency Information					
□	Medical/Health Information	□	Mental Health Information	□	Disability Information
□	Workers' Compensation Information	□	Patient ID Number	□	Emergency Contact Information
Device Information					
□	Device settings or preferences (e.g., security level, sharing options, ringtones)	□	Cell tower records (e.g., logs, user location, time, etc.)	□	Network communications data
Specific Information/File Types					
□	Personnel Files	□	Law Enforcement Information	□	Credit History Information
□	Health Information	□	Academic/Professional Background Information	□	Civil/Criminal History Information/Police Record
□	Case files	□	Security Clearance/Background Check	□	Taxpayer Information/Tax Return Information

PII/Data elements within CRMS varies based on user categories- including USDA employee and General Public. USDA employee information consist only of CRMS Administrator staff who handle complaints. The data elements will only consist of first name, last name, role, email and password to access the admin portal. Within CRMS the complaints are submitted by the General Public (complainants). The PII/Data elements shared within each complaint submission may include: Name, Date of Birth, Miscellaneous identifiers, Race, Ethnicity, Gender.

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

Federal employees & members of the public.

2.2.1. How is the information collected?

From individuals through the USDA Public Site (Salesforce Community Site) https://cloudapps2.my.salesforce.com/

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?

CRMS Forms will be designed with validation features to ensure completeness of submission including Address Validation tools to ensure address, state, congressional district info is correct. Program Complaint division physically reviews all complaints. In addition, there is a validation checklist created that validates (address, state, congressional district info). The form is uploaded into the system upon completion by staff.

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

Yes

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

Civil Rights Management System (CRMS)- USDA Salesforce Application built on USDA Salesforce Platform.

- Civil Rights Management System (CRMS) provides USDA with the ability to create, manage, track, and report on USDA CR Program complaints and cases, including but not limited to Title VI, Title IX, Section 504, and LEP.

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

CRMS utilizes third-party websites to conduct business for address and name verifications using U.S. Postal Service and/or Experian. The system currently has a license with Experian.

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of Information.

Follow the format below:

Privacy Risk: 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.

Mitigation: The CRMS application is housed on the USDA OCIO Salesforce Platform. The platform-level privacy and security controls will be adopted at the application level to ensure PII is safeguarded and handled properly under FEDRAMP guidelines. Application-level controls including establishing access roles, access levels across the system and logging into all system activities.

Section 3.0 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?

Complainant Information is used by USDA to review, process and approve the complainant case. The system creates, manages, tracks and report on USDA CR complaints and provides cases status. The information is used to generate official documentation to process the case which includes electronic approval or physical signature for documentation sent via mail.

3.2. Complaint information within the CRMS is shared across the Office of the Assistant Secretary for Civil Rights (OASCR) and the Mission Areas exclusively with employees who are part of the complaint management staff or leadership responsible for the CRMS program or compliance.

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.

Salesforce Service Cloud base features handle base data analytics. More advanced analytics are achieved through Salesforce Service Analytics and Tableau, which are Salesforce FedRAMP products. Tableau dashboards maintain CRMS data used for queries, reports and to respond to data calls.

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk: Associated Privacy act risks 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: Implementing the following actions, better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

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 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to use 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?

Notice will be provided to users prior to collection. The statement below is identified on the website, complaint form and electronic form.

CONSENT: This USDA Program Discrimination Complaint Form is provided in accordance with the Privacy Act of 1974 (5 U.S.C. §552a) and is used to solicit information for processing complaints of discrimination. The United States Department of Agriculture's Office of the Assistant Secretary for Civil Rights (OASCR) requests this information pursuant to 7 CFR Part 15. If the completed form is accepted as a complaint, the information collected during the investigation will be used to process your program discrimination complaint.

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

CRMS will only collect or consume the information submitted by the complainant and do not foresee any risks with individuals being unaware of the collection. The language below comes from the OMB approved USDA Program Discrimination Complaint Form.

PURPOSE: The information solicited on this form is used for processing complaints of discrimination under the statutes listed in the "Authorities" section of this notice. Any information obtained from this form will be maintained in our system of record.

DISCLOSURE: Providing this information is voluntary. Failure to complete this form may lead to a delay in processing the complaint or rejection of the complaint due to inadequate information to continue processing.

You may submit your completed form or letter to USDA by: Mail: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence, Ave, SW, STOP 9410, Washington, DC 20250-9410; Fax: 1 (833) 256-1665 or (202) 690-7442; or e-Mail: program.intake@usda.gov
If a user declines to provide information this may limit their ability to submit via online form due to required fields for submission. A complete case submission requires specific fields of information to be submitted on public-facing site including Name and Address. If a user declines, the alternative option to submit complaint via mail, fax or email can be provided.

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.

Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.

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 5.0 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?

Records are retained and disposed of in accordance with NARA’s General Records Schedule 16 and USDA’s General Records Schedule 2.3 but may be retained for a longer period as required by litigation, investigation, and/or audit. Electronic and/or paper records are retained with USDA employees at USDA offices.

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 indefinitely until NARA general record for program complaints are established. and disposed of in accordance with NARA’s General Records Schedule 16.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk: There is a risk of unauthorized exposure to the data. A privacy risk associated with CRMS is that the system will retain information (indefinitely) until NARA creates a record schedule for the system which can increase the likelihood of a data breach. The longer data is kept, the more opportunities there are for unauthorized access, leading to potential misuse of sensitive information.

Mitigation: The processes and activities for handling all active and non-active case records must be defined and monitored for compliance. In addition, all system users supporting processes must be trained on retention and handling of PII data and system access.

To mitigate the increased likelihood of data breach due to the system retaining information indefinitely, the system has been equipped with access controls such as limiting who can view or modify the data, and processes to protect against unauthorized access. To gain access to CRMS data, a specialist must receive three levels of approval, once access is granted, authorized users are reviewed quarterly.

Section 6.0 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?

The complaint information within CRMS is being shared across the OASCR and the Mission Areas with only those employees serving as complaint management staff or leadership responsible for CRMS program or compliance. Any CRMS generated reports or information can be shared via email, PDF, excel to fulfill the report requirements.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Complaint information is not securely handled even during internal information sharing. Unauthorized disclosure of complaint information

Mitigation: Ensure all internal team members are trained on safeguarding PII and unauthorized disclosure of complaint information.

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?

Information from CRMS is not transmitted to other external organizations. There are reports generated based on data within CRMS that are posted on the OASCR website for the general public to view.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: 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.

Non-compliance with Regulations: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Data Sharing Policy: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Section 7.0 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?

Internal OASCR Users: individuals will need to request access changes from the CRMS system administrator. All access profiles are maintained by eAuth and users can maintain their profiles through eAuth. Authorized CRMS users request access or updates to their CRMS account through their directors who sends the request for approval along with justification to the CRMS administrator for approval and access.

Complainant: USDA provides information on how to update the case record within the Acceptance Letter. Language from the letter:
If you do not agree with the defined claim(s) of your acceptance, you must provide us with sufficient reasons, in writing, within seven (7) calendar days of receipt of this letter. The statement should be sent to the following address, fax, or email:

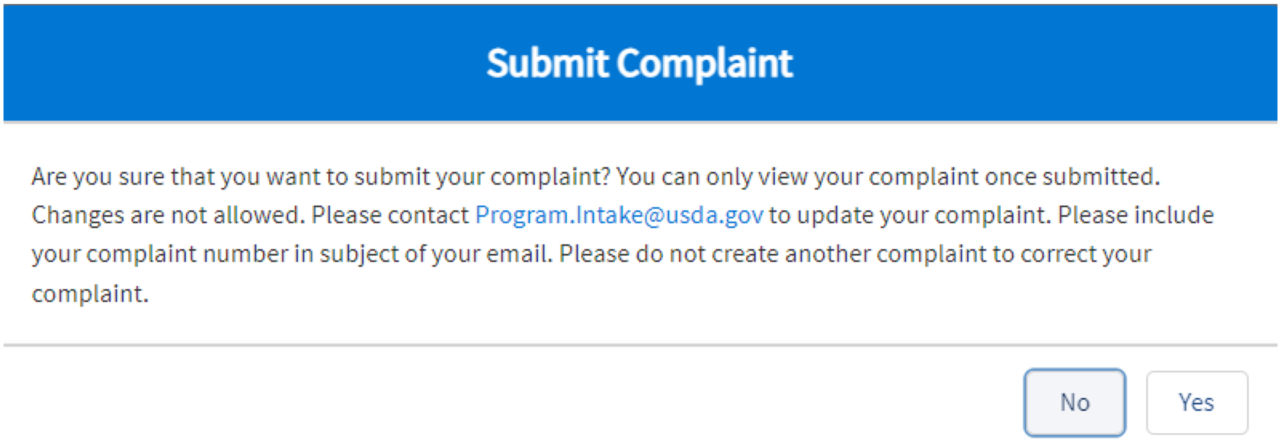
Program Intake Division
Center for Civil Rights Enforcement
United States Department of Agriculture
1400 Independence Avenue, SW
Stop Code: 9410
Washington, DC 20250
FAX: 833-256-1665
or
E-mail: ProgramComplaints@usda.gov

Also, complainants can check the status of their complaint at any time by logging into the CRMS public facing portal. It identifies the basis for the complaint, the program involved, date submitted and current step

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

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

The OASCR website Program Discrimination Complaint Filing | USDA provides contact email, phone and fax number to OASCR for further guidance on filling a discrimination complaint form. The public facing portal awaiting production has specific language that identifies how to update information in CRMS. Please see the information below that pops up when you select submit on the portal site.



Submit Complaint

Are you sure that you want to submit your complaint? You can only view your complaint once submitted. Changes are not allowed. Please contact Program.Intake@usda.gov to update your complaint. Please include your complaint number in subject of your email. Please do not create another complaint to correct your complaint.

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

N/A.

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: **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.

A potential mitigation would be to provide guidance on the website regarding how to update case records. *OASCR website and the CRMS public facing portal* provides guidance to individuals on how they can correct inaccurate or erroneous information collected about them.

To submit additional information or ask further questions, please call, email or fax the additional information/documentation.

Program Intake Division
Center for Civil Rights Enforcement
United States Department of Agriculture
1400 Independence Avenue, SW
Stop Code: 9410
Washington, DC 20250
FAX: 833-256-1665
or
E-mail: ProgramComplaints@usda.gov