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."
04/24/2025	1.2	Converted the PIA data to the new template

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	National Organic Program/Enforcement Tracking System
Program Office	National Organic Program
Mission Area	MRP
CSAM Number	2691
Date Submitted for Review	TBD

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Angela Cole	Angela.cole@usda.gov	(202) 465-6265
Information System Security Manager	Jorge Rios	Jorge.b.rios@usda.gov	(301) 851-2506
System/Program Managers	Lori Tortora	Lori.tortora@usda.gov	(202) 256-9964

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 National Organic Program’s (NOP) Enforcement Tracking System (NETS) replaced the existing Compliance and Enforcement Information Management System and is used to manage the intake, review and investigation of complaints regarding organic operations and organic labeling. Individuals submit complaints via an online portal, email, physical mail, or over the phone, and the information is tracked within NETS throughout the investigation. NETS collects the PII of the individuals submitting the complaints, the individuals who are the subject of the complaints, the individuals who provide information about complaints and the third-party organic certifiers who are responsible for certifying organic operations. This PII consists of their names, email addresses, phone numbers, home addresses, business addresses, business phone numbers and in some cases business financial information and financial account numbers (these may include sole proprietorships).

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 National Organic Program (NOP) Compliance & Enforcement Division (CED) ensures compliance of USDA organic regulations by investigating complaints of alleged violations, working with operations to achieve compliance where possible, and recommending enforcement actions, as appropriate. NOP staff gather information from individuals who file complaints with the NOP, individuals who are the subject of investigations, certifying agents, and individuals or agencies who provide information related to investigations. NETS is a case management system that offers tracking and workflow tools to support NOP enforcement activities. NETS receives around 500 complaints per year.

NETS receives certifier and operation point of contact information from the NOP Organic Integrity Database (OID). The system does not interface with systems external to NOP. NETS replaces a legacy system, the Compliance and Enforcement Information Management system, that also maintained complaint and investigation information. The information collected in NETS is authorized under the Organic Foods Production Act (OFPA) and the USDA organic regulations in 7 CFR Part 205.

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?

Enforcement provisions are included in the Organic Foods Production Act (OFPA) and the USDA organic regulations in 7 CFR Part 205.

The NOP accredits certifiers under the authority of the OFPA, as amended (OFPA; 7 U.S.C. 6501 et seq.). The compliance and enforcement provisions are found in 7 CFR 205.660 – 205.669 of the USDA organic regulations.

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

Yes

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

A SORN is currently in development and will be posted publicly once completed. A Plan of Action and Milestone (38876) was created for SORN.

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

Yes. The control number assigned to the information collection requirements in this part by the Office of Management and Budget pursuant to the Paperwork Reduction Act of 1995, is OMB number 0581–0191.

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)
☒ 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
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☒ Home Phone or Fax Number

☒ Home Address
☒ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☐ Military Service Information

☐ Race
☐ Nationality
☐ Mother's Maiden Name

☒ Personal Email Address
☐ Business Email Address
☐ Global Positioning System (GPS)/Location Data

☐ Employment Information
☐ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☐ Education Information
☐ Resume or Curriculum Vitae
☒ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

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

Characteristics

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

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

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

[List additional information collected but not listed above here (for example, a personal phone number that is used as a business number).]

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

Individuals who submit complaints are the source of both their own information and the information on the subjects of the complaints. This consists of their names, email addresses, phone numbers, home addresses, business addresses and business phone numbers.

NOP staff will also gather information from public online sources, business websites or direct contact with individuals or businesses during the complaint investigation to supplement any missing information or to confirm the accuracy of information submitted by the individuals who submitted a complaint. This information consists of names, email addresses, phone numbers, addresses, business addresses and business phone numbers.

Information about organic operations and third-party organic certifiers is also obtained from NOP's OID. This information consists of the names, email addresses, phone numbers, business addresses and business phone numbers of the points of contact regarding the operations.

During the investigative process, the organic certifiers sometimes provide financial account information of the businesses that are the subject of investigations. This information may be needed to understand if any fraud has occurred, such as a business selling organic products while suspended or selling more organic product than could be produced by a farm or business.

2.2.1. How is the information collected?

Individuals who submit complaints provide their own information and information on the subjects of the complaints (names, email addresses, phone numbers, addresses, business addresses and business phone numbers) during the complaint submission process, using the following methods:

- NOP Online Complaint Portal
- Email: NOPCompliance@usda.gov
- Phone: 202-720-3252
- Fax: 202-720-3552

If received by the Online Complaint Portal, the information is submitted directly to NETS.

If received by email, phone, or fax, NOP staff enter the information into the Online Complaint Portal themselves and submit directly into NETS.

Additionally, during the investigation process, NOP staff gather information through research (e.g., website searches, contacting businesses directly via phone or email) to supplement any missing information and confirm the information provided by the complainants (names, email addresses, phone numbers, addresses, business addresses and business phone numbers). They also use this research to collect additional address and point of contact information for federal, state or local programs overseeing regulated entities, and external organizations (i.e., agricultural businesses and NOP accredited certifiers) who submit the financial information of organic operations do so using Cloud Vault or encrypted email.

NOP staff will also reference the organic operation and certifier entity information within the NOP OID to supplement missing information or confirm information (names, email addresses, phone numbers, addresses, business addresses and business phone numbers of the representatives of the organic operations or the certifiers). In these cases, the NOP staff will use the information in the OID to manually input or update the information in NETS.

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

During the investigation process, NOP staff gather information through internet research and collect additional address and point of contact information for federal, state or local programs overseeing regulated entities, and external organizations (i.e., agricultural businesses and NOP accredited certifiers). NOP staff will also review publicly available websites, including business websites, to confirm contact information submitted by complainants.

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

NOP staff verify the information directly with the individuals who provided the information in the complaint and verify business information via internet searches and by referencing the USDA's OID. The NOP Compliance and Enforcement Division (CED) has standard procedures for complaint intake and conducting investigations, which includes confirming the accuracy of information submitted.

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

No

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:

There is a risk that more information will be collected than necessary. There is also a risk of inaccurate information, especially in cases where the complainant is providing the information on the subjects of complaints.

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?

Information in NETS is used by NOP staff to track inquiries, complaints, correspondence, and enforcement activities throughout an enforcement investigation lifecycle. The PII collected and maintained in the NETS system is used to contact individuals or businesses to get additional information to investigate complaints so NOP staff can enforce NOP regulations. The business financial information is used by NOP investigators to understand if a business committed organic-related fraud.

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.

NETS is not used to conduct predictive analysis or discover any patterns in data.

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 System of Record Notice (SORN) and Privacy Act Statement are currently being developed and will provide notice to individuals on how and why their information is processed. Additionally, the instructions for how to file an organic complaint that are posted online include a basic statement of how and why PII is collected as part of the complaint process.

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

The online complaint form includes an option to remain anonymous. If users select this option, they can still submit a claim without providing any PII. Individuals who choose to remain anonymous are presented with a message that informs them that the USDA will not be able to contact or update them about their submission.

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

Follow the format below:

Privacy Risk:

There is a risk that individuals will not be aware of why their information is collected or what the USDA will do with it.

Mitigation:

A Privacy Act Statement and SORN are in development and will provide full notice of how and why the information collected will be used by the USDA. Additionally, users are presented with a disclaimer when filling out a compliant about the confidentiality of their information and the option to remain anonymous: “The identities of complainants will be considered confidential and will be protected to the greatest extent permissible by law.”

Individuals submitting complaints may choose not to submit PII. Any PII submitted is protected under the authority of 7 U.S. Code § 6519(a)(5) confidentiality provisions.”

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?

The NOP electronic records file plan is currently under review. PII will be retained permanently, until a records file plan is approved. According to the draft plan, compliance and enforcement case files are considered temporary and will be destroyed 5 years after the end of the fiscal year in which the final action is taken, or the case is closed.

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.

No. The NOP is currently working with the AMS Records Officer for NARA approval of the NOP Records File Plan.

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

Follow the format below:

Privacy Risk:

All the information in NETS is currently stored indefinitely, until a records file plan for enforcement case files is approved. The indefinite storage of information raises the risk of unauthorized access or disclosure the longer it is held.

Mitigation:

The risk is reduced by only NOP authorized users having access to the system and the information being retained for retention purposes. The proposed 5-year retention period balances the occasional need to access historical data for compliance and enforcement analysis with the understanding that information cannot be retained indefinitely to protect the privacy of individuals.

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?

The information in NETS is primarily used for internal investigations within NOP. In cases of appeals, Freedom of Information Act (FOIA) requests, and judicial actions, information will be shared as necessary with the relevant oversight agencies, such as the USDA Office of General Counsel. The name and email of a complainant, if submitted by the complainant, are shared with oversight agencies as part of the administrative case file. Additionally, case files, including PII, will be shared within USDA when it is necessary for litigation and any agency within USDA (or any employee of USDA in their official capacity) is a party to the litigation or has a legitimate interest in the litigation. All the information shared internally is transmitted through encrypted email. PII contained in case file records is also saved on the USDA SharePoint to allow for more efficient review and compilation of documents related to a case. Access in SharePoint is limited only to NOP Compliance and Enforcement staff who have a need-to-know.

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

Follow the format below:

Privacy Risk:

There is a risk of unauthorized access to the data during internal sharing.

Mitigation:

Data is only shared upon request as required by regulations and enforcement actions. Information is emailed using encryption to staff that do not have access to NETS only for the purposes listed. Only NOP authorized users have access to the PII in NETS. Access to case files that are stored on the internal USDA SharePoint is limited only to NOP Compliance and Enforcement staff who have a need to know.

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?

Case files, including the names and contact information for those involved in organic investigations, will be shared outside of the USDA when it is necessary for the litigation of organic regulations. This includes sharing information with the U.S. Department of Justice or other Federal or state agencies conducting litigation or in proceedings before any court, adjudicative or administrative body. Case files shared externally are transmitted through encrypted email.

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: 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: 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 do not have direct access to the NETS after submitting an online complaint. However, individuals can contact the NOP via email or phone to verify or change their personal contact information using the following contacts:
Email: NOPCompliance@usda.gov
Phone: 202-720-3252
Fax: 202-205-7808
Mail: NOP Compliance and Enforcement Branch
Agricultural Marketing Service
United States Department of Agriculture
1400 Independence Avenue, S.W.
Mail Stop 0268, Room 2642-S
Washington, D.C. 20250-0268

Individuals may also submit a Freedom of Information Act (FOIA) request or Privacy Act Request to access their information using the following contact information:
FOIA Officer
1400 Independence Avenue, SW
Room 2055-S, Stop 0201
Washington, DC 20250-0201
Tel. (202) 302-0650
E-Mail – AMS.FOIA@usda.gov

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

Individuals can contact the NOP to verify or change their personal contact information as listed above. Additionally, individuals may submit FOIA or Privacy Act Requests as listed above.

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

NOP is unable to contact individuals if the individual does not provide contact information. If an individual does provide their contact information, they can contact the NOP any time via email or phone to update their information. The online complaint submission screen provides email and phone numbers to contact NOP. If an individual provides an email address when they submit a complaint, confirmation of complaint receipt is sent via email to them with contact information for NOP which can be used to submit requests to access or correct information. Additionally, contact information for the NOP is listed publicly on NOP's website. The procedures for submitting FOIA or Privacy Act requests are posted publicly online on AMS' website.

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

A formal redress process is provided as listed above.

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

Follow the format below:

Privacy Risk:

There is a risk that individuals will not be able to or aware of how to access or correct their PII.

Mitigation: Individuals are provided with options to access or update their information directly with the NOP and through FOIA and Privacy Act Requests. Individuals are provided with contact information to submit these requests on the NOP website, in the email confirmation that they receive after submitting a complaint and on the AMS website.

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?

The PII in NETS is protected with encryption which ensures that information will not be readable to unauthorized individuals. Access to the NETS requires multi-factor authentication, requiring a password and an additional form of authentication. NOP personnel and contractors are required to complete USDA Information Security Awareness Training prior to gaining access to the system and annually thereafter. Access to data in the system is controlled by user roles which are assigned appropriately to end users with permissions to view and edit data based on their role. User approval and removal requests are provided by the NETS system owner. The NETS system owner has access to an "Audit Log" feature that provides information on who is logged in and when users are logged in. The audit log also records when data information is modified and the user that modified the data. The audit logs are available to be reviewed if information in the system is compromised.

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

Access to data in the system is controlled by user roles which are assigned appropriately to end users with permissions to carry out functions within the system based on role. New NETS users require supervisor approval for access to the system, and the NETS system owner determines access and roles for users. The user access list will be reviewed several times a year by the NETS system owner to ensure that access remains relevant and appropriate. The process for providing access to NETS and reviewing existing access is documented in internal procedures.

Access to the SharePoint files is limited to NOP staff only and is managed by the Compliance and Enforcement Division (CED) SharePoint Site owner. Any exceptions to access require the NOP's CED management approval and are documented in the CED SharePoint Governance Plan. The list of users who have access to SharePoint is reviewed on a quarterly basis by the NOP Quality Manager to ensure that access remains appropriate. The process for granting access to the SharePoint files and reviewing access on a quarterly basis is documented in the CED SharePoint Governance Plan.

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

The NETS System Owner and the Director of the NOP Compliance and Enforcement Division reviews and approves information sharing requests. NOP shares PII information when it is necessary for case violations that result in litigation or other Federal, State, local, international law enforcement agency investigations, or Federal agencies conducting litigation or are in proceeding before any court, adjudicative, or administrative body.

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

All users are USDA/NOP Staff or support contractors and are all required to take the USDA's annual information security awareness training.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 6/12/2025

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

Signed:_____

Signature of Responsible Officials

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

Signed: LORI TORTORA Digitally signed by LORI TORTORA Date: 2025.07.23 11:05:30 -04'00'

Lori Tortora
NOP NETS System Owner
National Organic Program, Compliance and Enforcement Division
U.S. Department of Agriculture

Signed: ANGELA COLE Digitally signed by ANGELA COLE Date: 2025.07.25 14:38:40 -04'00'

Angela Cole
Assistant Privacy Officer/ Assistant Chief Information Security Officer (acting)
Marketing and Regulatory Programs
U.S. Department of Agriculture

Signed: TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.07.14 08:45:01 -04'00'

Office of the Chief Privacy Officer
U.S. Department of Agriculture