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.”
6/6/2025	1.1	Review and Updated – Christiana North

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	OHS Foreign National Vetting Application
Program Office	Office of Homeland Security
Mission Area	Departmental Administration Information Technology Office
CSAM Number	2623
Date Submitted for Review	June 6, 2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Nija Enclarde	nija.enclarde@usda.gov	318-955-1393
Information System Security Manager	Lisa M. McFerson	lisa.mcferson@usda.gov	202-720-8599
System/Program Managers	Carrie, Moore	carrie.moore@usda.gov	202-720-3487

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 Office of Homeland Security’s (OHS) Foreign National Vetting (FNV) application (App) supports the risk assessment process on foreign nationals (non-U.S. Persons) who visit or perform work at United States Department of Agriculture (USDA) facilities in the United States. This Privacy Impact Assessment (PIA) is being conducted to identify the risks and potential effects of collecting, maintaining, and disseminating the required Personal Identifiable Information (PII) needed to conduct the risk assessment and to mitigate potential privacy risks.

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 Secretary of Agriculture, in accordance with 7 Code of Federal Regulations (CFR) §2.95, has delegated responsibility for matters relating to counterintelligence (CI) and insider threats to The Office of Homeland Security (OHS). Within OHS, those Programs fall under the National Security Division (NSD). The high-level strategic goal of NSD is to counter threats to the Department with the objective to execute activities to detect, deter, and protect against espionage, insider threats, and external adversaries per Departmental Regulation (DR) 4600-003, USDA Defensive Counterintelligence and Insider Threat Programs, released on July 12, 2021.

The objective of FNV is to identify any risks from a national security, counterintelligence, or anti-terrorism perspective prior to granting a foreign national (non-U.S. Person) access to the Department’s facilities, personnel, programs, information, and systems. USDA is mandated by Executive Order (E.O.) 12977, Interagency Security Committee (ISC), to protect Government property and facilities; restrict access to certain areas and materials; protect sensitive and Controlled Unclassified Information (CUI); and ensure the health, safety, and security of Federal and non-Federal employees in our facilities. ISC released Facility Access Control, An Interagency Security Committee Best Practice, in 2020 that includes guidance on FNV and foreign access management.

The OHS FNV App with Salesforce provides a centralized, departmentwide tracking system for agencies and staff offices to submit vetting requests on foreign nationals (non-U.S. Persons only) entering USDA facilities in accordance with DR 4600-004, Foreign Visits and Assignments Vetting, and provides stats on the FNV program for dashboard reporting to leadership.

Designated agency points-of-contact will submit the necessary identifying information on a foreign national into the OHS FNV App. OHS is automatically notified of the submission, conducts a quality check, and enters the information into the Counterintelligence Threat Actor Discovery Exploitation Landscape (CITADEL) managed by the Office of the Director of National Intelligence (ODNI). ODNI is our service provider for foreign national screening. The CITADEL vetting result is received and entered into the OHS FNV App. The agency requestor and designated Host/Supervisor, receives an automatic notification of the determination.

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?

In order to conduct the appropriate record checks through CITADEL, PII relating to the identity of the foreign national is obtained. Authorities associated with protecting federal assets and countering foreign threats include:

- 7 CFR § 2.95, Director, Office of Homeland Security
- DR 4600-003, USDA Defensive Counterintelligence and Insider Threat Programs, July 12, 2021
- DR 4600-004, Foreign Visits and Assignments Vetting, May 27, 2021
- DHS, Cybersecurity and Infrastructure Security Agency, Interagency Security Committee, Facility Access Control, An Interagency Security Committee Best Practice, 2020 Edition
- E.O. 12977, Interagency Security Committee, October 19, 1995
- Memorandum of Agreement (MOA) between the Department of Homeland Security (DHS), Office of the Chief Security Officer, and the United States Department of Agriculture (USDA), OHSEC, December 15, 2016
- National Security Presidential Memorandum (NSPM) 33, United States Government- Supported Research and Development National Security Policy, January 14, 2021
- Office of the Director of National Intelligence (ODNI), National Counterintelligence Strategy for the United States of America, 2024
- ODNI, Annual Threat Assessment, March 2025

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

The system has completed the certification and authorization process, receiving an Authority to Operate (ATO) dated 8/10/2022. The system is hosted on Salesforce, a FEDRAMP approved system, approved for use with multiple USDA agencies.

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

GOVT-1: General Personnel Records SORN https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnelrecords.pdf

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

Yes, information is covered by the Paperwork Reduction Act.

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

☐ 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

Personnel Type (Research Assignment, Advisory Board, Contractor, or Visitor)

Purpose of Visit/Arrangement

Foreign National's Name

Foreign National's Email

Immigration Info (Visa info, foreign passport info, or Permanent Resident Card info)

Foreign National's Employer or University Name

Foreign National Phone Number

USDA Facility Name, City, State

Projected Arrival/Departure Dates

USDA Host/Supervisor Name, Email

USDA User/Requestor Name, Email

USDA Agency for Staff Office

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

The information is entered into the system by an agency user, typically within Human Resources or Personnel Security, who is with the USDA agency that is sponsoring or employing the foreign national. The information is obtained from various forms completed for the background investigation process, such as Standard Forms (SF) questionnaires (SF85 and SF85P) and Optional Form 306 (Declaration for Federal Employment), as well as exchange visitor forms, and other research collaboration documents.

2.2.1. How is the information collected?

The USDA agency sponsoring the visit collects information regarding the foreign national from the individual. The USDA agency hiring or onboarding a federal employee or non-fed (contractor, consultant, etc.) collects information regarding the foreign national from the background investigation questionnaire handled by Human Resource or Personnel Security offices, or agency international visitor offices.

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

The system does not use commercial or publicly available data.

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

Information collected will be verified for accuracy by the sponsoring agency against information and documents collected directly from foreign nationals, to include any foreign passport or visas.

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?

Not Applicable – There are no third-party websites in use with the application.

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

PII does not cross third party websites

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

Follow the format below:

Privacy Risk: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

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

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 information in the OHS FNV App is collected and used to prepare and conduct a risk-based national security assessment on a foreign national seeking access to USDA in accordance with DR 4600-004, Foreign Visits and Assignments Vetting. The information is shared with CITADEL to conduct foreign national screening services to identify any adverse information.

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.

There are no data analysis tools, but the OHS FNV App does collate information to produce stats for dashboard reporting. Only tools used to analyze data are out of the box Salesforce reporting and Dashboards.

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

Follow the format below:

Privacy Risk: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Mitigation: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

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?

Notice is provided to the individual prior to collection of information. For example, the Standard Forms (SF) include a routine uses statement that includes, “To Executive Branch Agency insider threat, counterintelligence, and counter terrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards.” The Optional Form (OF) 306, Declaration for Federal Employment, includes a routine uses statement that includes, “Federal agencies, or other sources requesting information for Federal agencies, in connection with hiring or retaining, security clearance, security or suitability investigations.

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

The SF forms inform the individual that the information collected may be disclosed without their consent as permitted by the Privacy Act (5 USC 552a(b)) and under the routine uses (see 6.2 for related routine use).

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

Follow the format below:

Privacy Risk: Not adequately informing individuals about changes to privacy practices or policies can lead to confusion and mistrust, especially if data practices evolve.

Mitigation: Train employees on data protection practices and the importance of privacy notices to ensure compliance and proper handling of personal data.

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?

Information on FNV is retained in accordance with NARA General Records Schedule 5.6: Security Records, dated April 2020 under Item 230 covering insider threat and counterintelligence information.

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.

NARA General Records Schedule 5.6: Security Records.

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

Follow the format below:

Privacy Risk: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

Mitigation: Ensure that employees are aware of and trained on the data retention policy, including the importance of compliance and the procedures for handling personal information.

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 details and PII contained within a FNV request is only accessible within the OHS FNV App by approved agency users across all USDA agencies and offices who have foreign nationals visiting or on assignments that require vetting in accordance with DR 4600-004. This information is not further shared internally.

Statistics are collated and shared via dashboards and in annual program reports, such as the total number of FNV requests completed, requests by agency, etc., to report on program status, accomplishments, and other areas of interest. Annual reports are shared by the OHS Director with the Assistant Secretary for Administration (ASA) up to the Office of the Secretary (OSEC) and may go to additional senior leaders across the Department. No PII is shared in this effort.

Dashboard data (does not contain PII) in the OHS FNV App may be shared via the Department's Enterprise Data Analytics Platform & Toolset (EDAPT) platform.

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

Follow the format below:

Privacy Risk: Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Mitigation: Implement role-based access controls to limit who can access PII based on their job responsibilities.

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?

The information collected for the FNV request is shared with ODNI in CITADEL. ODNI is USDA's service provider for conducting record checks on foreign nationals. The information is manually entered directly into CITADEL by an OHS FNV App Admin user. ODNI provides user access to CITADEL.

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

Follow the format below:

Privacy Risk: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.

Mitigation: Develop an incident response plan that outlines procedures for addressing potential data breaches or unauthorized disclosures related to external sharing.

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?

Pursuant to the Privacy Act, individuals can access information they have provided to USDA. Privacy Act requests are submitted online through the USDA Public Access Link (PAL). PAL allows you to create, submit, and track the status of your Freedom of Information Act (FOIA) request(s). The FOIA is found in Title 5 of the United States Code, Section 552. Reference §1.3 Requirements for Making a Request for our FOIA Regulations.

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

Any individual who wishes to request correction or amendment of any record pertaining to him or her contained in a system of records maintained by an agency shall submit that request in writing to the owner of the information in accordance with USDA requirements at §1.116 Request for correction or amendment to record.

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

Notice to individuals about policies regarding the collection, use, and disclosure of information are provided on the forms at the time the information is collected, and that information includes procedures on correcting their information. Human Resources representatives provide employees with procedures for correcting their information. Individuals are provided notice via the privacy policy, the related system of records notices (SORNs), and the related Privacy Impact Assessments (PIA), including this one.

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

Not Applicable – formal redress is provided

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

Follow the format below:

Privacy Risk: 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.

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

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 data is restricted to only approved personnel, who will only be able to access the system using a USDA PIV card and government computer. All Data is Encrypted using 256-bit Advanced Encryption Standard (AES), safeguarding unauthorized access to data in the backend.

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

OHS FNV App user accounts are individually approved by OHS Insider Risk Program Manager and meet vetting, training, and limited access requirements as outlined in section 1.7. Instructional information is provided in OHS FNV App Admin Guide and additional procedures are provided in Departmental Guide (DG) 4600-004, Foreign Visits and Assignments Vetting Procedures.

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

The information collected for the FNV request is shared with ODNI in CITADEL. ODNI is USDA's service provider for conducting record checks on foreign nationals.

CITADEL is a centralized repository of counterintelligence and National Security Threat Actor (NSTA) information. No U.S. Person information/data is collected. ODNI completed Privacy Analysis Worksheets (PAW) on CITADEL, both on the unclassified system version and the classified system version, on January 11, 2021, that determined no PIA or SORN was required as it is not a Privacy Act System of Records. The PAW is classified.

External sharing with ODNI/CITADEL has protections in place to mitigate risks in the PAWs completed in January 2021.

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

All information system users are required to take mandatory security awareness training with PII training before being granted access to the system and at least annually thereafter.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 6/23/2025

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

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.07.14 16:52:59 -04'00'

Signed:_______________________________________

Signature of Responsible Officials

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

Signed:_______________________________________

Marcia Moore
System Owner
Office of Homeland Security
U.S. Department of Agriculture

Signed:_______________________________________

Nija Enclarde
Mission Area Privacy Officer
Departmental Administration Information Technology Office
U.S. Department of Agriculture

Signed:_______________________________________

Sullie Coleman
ACISO
Departmental Administration Information Technology Office
U.S. Department of Agriculture