Privacy Impact Assessment
Template

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: May 21, 2015
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Office of Homeland Security
Foreign National Vetting Application
(OHS FNV App)

March 1, 2022

Contact Point

Carrie Moore
National Security Division
Office of Homeland Security
202.720.3487

Reviewing Official

Michele Washington
Privacy Officer
United States Department of Agriculture
(202) 205-3369

Abstract

The Office of Homeland Security's (OHS) Foreign National Vetting (FNV) application (app) supports the risk assessment process on foreign nationals (non-U.S. citizens) 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 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 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 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 entering USDA facilities in the U.S. in accordance with DR 4600-004, *Foreign Visits and Assignments Vetting*, and provides stats on the FNV program for dashboard reporting to leadership. USDA has a Memorandum of Agreement (MOA) with the Department of Homeland Security (DHS) to conduct our foreign national screening.

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 DHS Integrated Security Management System (ISMS)/Foreign Access Management System (FAMS). The DHS 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 1.0 Characterization of the Information

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

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

The information collected in the OHS FNV App for a foreign vetting request include:

- Personnel Type (Fed Employee, Research Assignment, Advisory Board, Contractor, or Visitor)
- Foreign National's Name
- Foreign National's Email
- Foreign National's Date of Birth
- Foreign National's Race
- Foreign National's Sex
- Foreign National's Place of Birth
- Foreign National's Country of Citizenship
- Immigration Info (Visa info, foreign passport info, or Permanent Resident Card info)
- Foreign National's Employer or University Name
- USDA Facility Name, City, State
- Projected Arrival Date
- USDA Host/Supervisor Name, Email
- USDA User/Requestor Name, Email
- USDA Agency or Staff Office

1.2 What are the sources of the information in the system?

The information is entered into the system by an agency user, typically within Human Resources or Personnel Security, who are 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.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information in the OHS FNV App is collected and used to prepare and conduct a risk-based assessment on a foreign national seeking access to a USDA facility in the United States in accordance with DR 4600-004, *Foreign Visits and Assignments Vetting*. The

information is shared with DHS to conduct foreign national screening services to identify any adverse information.

1.4 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.

1.5 How will the information be checked for accuracy?

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

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

In order to conduct the appropriate record checks maintained by DHS and other organizations across the Intelligence Community, 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*, 2020-2022
- ODNI, National Counterintelligence and Security Center (NCSC), *Countering Foreign Intelligence Threats: Implementation and Best Practices Guide*, June 2017

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk associated with the handling of PII on foreign nationals and application security risks. Privacy risks associated with the handling of PII could occur when data is extracted from the system and is improperly distributed or stored. There is always potential for an insider threat. An insider threat is when someone uses their authorized access, wittingly or unwittingly, to do harm to the security of the Department or the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

Mitigation: To minimize risks these risks, the following strategies are in place:

- The OHS FNV App can only be accessed via a LincPass for eAuthentication;
- User access will be restricted to individual's whose duties include processing visitor requests or background investigations for work with, or on behalf of, USDA or whom have a related need-to-know;
- User access to the OHS FNV App will be limited to records within their own agency or mission area;
- Only users who will be required to submit a FNV request will require access to the OHS FNV App;
- Automated email notifications have been established within the OHS FNV App to eliminate the need for Hosts/Supervisors to access the OHS FNV App for results;
- Administrator access is limited to the OHS Insider Threat Program Manager, the FNV Liaison position, and a backup;
- Any report downloaded from the OHS FNV App will be password protected to prevent unauthorized access;
- OHS FNV App user accounts are individually approved by the OHS Insider Threat Program Manager;
- All users receive mandatory annual Information Security Awareness training;
- All users have been vetted and found suitable, at a minimum, for a Public Trust position;
- All data within the application environment is hosted in a secure FedRamped Gov Cloud Salesforce Server.
- Specific security roles have been defined and implemented within the application to control access to information; and
- A system security certification was performed and obtained in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources
- All Data is Encrypted using 256-bit Advanced Encryption Standard (AES)

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The PII information is collected in order to conduct FNV to identify any risks from a national security, counterintelligence, or anti-terrorism perspective prior to granting a foreign national access to the Department's facilities, personnel, programs, information, and systems. This information is needed in order to conduct the appropriate record checks maintained by DHS and other organizations across the Intelligence Community. The information in the OHS FNV App will allow for tracking and statistical reporting on the FNV program to leadership.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Same as information provided under Section 1.7.

Section 3.0 Retention

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

3.1 How long is information retained?

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.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

NARA, *General Records Schedule 5.6: Security Records*, was updated in July 2017 to include insider threat information following Executive Order 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risks associated with the retention of this information is the possible dissemination of PII to unauthorized persons. This risk is mitigated per Section 1.7.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

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 assignment 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.

4.2 How is the information transmitted or disclosed?

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.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There are no risks associated with internal sharing of this information because PII is not contained in our statistical reporting.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

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

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

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), December 15, 2016

DHS-ALL-PIA-048 Foreign Access Management System of Records Notice (SORN)

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information is entered directly into the DHS Foreign Access Management System (FAMS) by an OHS FNV App Admin user. DHS provides direct system access to the FNV program.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

External sharing with DHS FAM Program has protections in place to mitigate risks in the DHS FAM 2011 and 2017 Privacy Impact Assessments and DHS-ALL-PIA-048 Foreign Access Management System of Records Notice (SORN).

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

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

6.2 Was notice provided to the individual prior to collection of information?

Yes, 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..."

6.3 Do individuals have the opportunity and/or right to decline to provide information?

The various forms collecting the information inform the individual the information is voluntary; however, a proper investigation may not be able to be completed if the information is not provided, which may affect their placement or employment prospects with USDA.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The SF forms inform the individual 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).

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Routine uses of information are stated on forms. This PIA serves as an additional notice on the receipt and use of this data for FNV purposes.

Section 7.0 Access, Redress and Correction

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

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 of 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: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Not Applicable - there are no privacy risks associated with the redress available to individuals.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

OHS FNV App user accounts are individually approved by OHS Insider Threat 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 will be provided in the Departmental Manual (DM to accompany DR 4600-004.

8.2 Will Department contractors have access to the system?

USDA contractors will have access to the system.

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

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

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Salesforce is a FEDRAMP approved system, approved for use with multiple USDA agencies.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Auditing Measures:

The system has auditing capabilities that stamps who, when, and what changes were made to a given record. This can also be elevated to track and audit certain fields. This can show who modified the field, what it was changed to, and when. Periodic reviews are conducted on the application of user roles and administrative actions are conducted by the OHS FNV App team.

Technical Safeguards

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.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There are minor risks associated with the handling of PII and system security. Privacy risks associated with the handling of PII could occur when data is extracted from the system and is improperly distributed or stored. There is always potential for an insider threat. An insider threat is when someone uses their authorized access, wittingly or unwittingly, to do harm to the security of the Department or the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

Mitigation: To following controls and mitigation strategies address these risks:

- The OHS FNV App can only be accessed via a LincPass for eAuthentication;
- User access will be restricted to individual's whose duties include processing visitor requests or background investigations for work with, or on behalf of, USDA or whom have a related need-to-know;
- User access to the OHS FNV App will be limited to records within their own agency or mission area;
- Only users who will be required to submit a FNV request will require access to the OHS FNV App;
- Automated email notifications have been established within the OHS FNV App to eliminate the need for Hosts/Supervisors to access the OHS FNV App for results;
- Administrator access is limited to the OHS Insider Threat Program Manager, the FNV Liaison position, and a backup;
- Any report downloaded from the OHS FNV App will be password protected to prevent unauthorized access;
- OHS FNV App user accounts are individually approved by the OHS Insider Threat Program Manager;
- All users receive mandatory annual Information Security Awareness training;
- All users have been vetted and found suitable, at a minimum, for a Public Trust position;
- All data within the application environment is hosted in a secure FedRamped Gov Cloud Salesforce Server. Specific security roles have been defined and implemented within the application to control access to information; and
- A system security certification was performed and obtained in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources
- All Data is Encrypted using 256-bit Advanced Encryption Standard (AES)

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

OHS will be utilizing Salesforce to build out and host an application to track and vet foreign nations. This will be utilizing PaaS (platform as service), as we are utilizing salesforce platform to build out software for OHS.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. All data will be hosted on Salesforce FEDRAMP Gov Cloud Servers, which have implementations to ensure all data is secure. OHS, along with DSC have put in place business procedures to only grant access to data to authorized personnel.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

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

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not Applicable – PII does not cross third party websites

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable – PII does not cross third party websites

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable – PII does not cross third party websites

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable – PII does not cross third party websites

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable – PII does not cross third party websites

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable – PII does not cross third party websites

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable – PII does not cross third party websites

10.10 Does the system use web measurement and customization technology?

Not Applicable – PII does not cross third party websites

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not Applicable – PII does not cross third party websites

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites

and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable – PII does not cross third party websites

Responsible Officials

CARRIE MOORE Digitally signed by CARRIE MOORE
Date: 2022.03.16 09:48:21 -04'00'

Carrie Moore, Project Manager, Office of Homeland Security (OHS)

United States Department of Agriculture

MATTHEW ALLEN Digitally signed by MATTHEW ALLEN
Date: 2022.03.16 13:06:23 -04'00'

Matt Allen, System Owner, Chief, OHS

United States Department of Agriculture

Approval Signature

Michele Washington
Privacy Officer
United States Department of Agriculture