



U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer



**FOREIGN LABOR
CERTIFICATION SYSTEM
FLAG
PRIVACY IMPACT ASSESSMENT**

VERSION 3.0

1/30/2023

DOCUMENT CHANGE HISTORY

Date	File name / Version#	Author	Revision Description
5/14/2020	1.0	S Parker	Update PIA into new Template for ATO
7/19/2021	2.0	S Parker	Annual Review, removed references to iCert and ETA GSS
12/12/2022	3.0	Mary Ford	Updated Questions throughout the document Updated Retention Completed Appendix B
12/19/2022	3.0	Mary Ford	Included FLAG
1/30/2023	3.0	Rekha Vayuvegula	Removed references to PERM

DOCUMENT REVIEW HISTORY

Date	Version#	Reviewers
05/14/2020	1.0	S Parker
07/19/2021	2.0	S Parker
12/14/2022	3.0	Kristina Mena
1/30/2023	3.0	John Chen
2/06/2023	3.0	John Chen

TABLE OF CONTENTS

Privacy Impact Assessment Questionnaire	4
1.1 Overview	4
1.2 Characterization of the Information.....	5
1.3 Describe the Uses of the PII.....	6
1.4 Retention	7
1.5 Internal Sharing and Disclosure.....	8
1.6 External Sharing and Disclosure	9
1.7 Notice.....	11
1.8 Individual Access, Redress, and Correction	12
1.9 Technical Access and Security	13
1.10 Technology	15
1.11 Determination	16
1.12 PIA Signature Page	17
 Appendix A: Definition for PII and PII Elements.....	 18
 Appendix B C: FLCS FLAG SYSTEM TRACKING TEMPLATE	 23

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

(To be completed for information systems containing PII)

1.1 OVERVIEW

FLCS FLAG

A Privacy Impact Assessment (PIA) is being conducted because the system stores and processes Personally Identifiable information (PII) of non-citizens seeking permanent employment. The PII collected includes non-citizen (applicant) names, dates of birth, addresses, government-issued identifiers, personal phone numbers, work experience and educational / work / training records.

The legal authorities to operate the program or system include:

- Immigration and Nationality Act, as amended, 8 U.S.C. 1101(a)(15)(H)(i), and (ii), 1184(c), 1182(m) and (n), 1182(a)(5)(a), 1188, and 1288. Section 122 of Pub. L. 101 - 649. 8 CFR 214.2(h). 20 CFR 655 Subpart A. 20 CFR 655.9; and
- Privacy Act of 1974

FLCS FLAG

The Foreign Labor Certification System - Foreign Labor Application Gateway (FLCS-FLAG) system modernized the legacy iCert system in order to reduce labor certification processing times and improve Office of Foreign Labor Certification (OFLC) decision quality and consistency. It utilizes multiple cloud-based platforms to enhance performance, scalability, and allow the inclusion of other Federal agencies as data stakeholders in OFLC business process workflows thus, eliminating a fragmented, stove-piped representation of Federal government services to citizens.

In FY 2023, FLCS-FLAG will start accepting permanent labor certification applications and begin the process of supplanting / decommissioning the legacy PERM Case Management System.

The Office of the Chief Information Officer operates and maintains FLCS- FLAG on behalf of the Office of Foreign Labor Certification, under DOL Ongoing Authorization (OA) program.

A Privacy Impact Assessment (PIA) is being conducted because the system stores and processes Personally Identifiable information (PII) of non-citizens seeking permanent employment. The PII collected includes non-citizen (applicant) names, dates of birth, addresses, government-issued identifiers, personal phone numbers, work experience and educational / work / training records.

The legal authorities to operate the program or system include:

- Immigration and Nationality Act, as amended, 8 U.S.C. 1101(a)(15)(H)(i), and (ii), 1184(c), 1182(m) and (n), 1182(a)(5)(a), 1188, and 1288. Section 122 of Pub. L. 101 - 649. 8 CFR 214.2(h). 20 CFR 655 Subpart A. 20 CFR 655.9; and
- Privacy Act of 1974

1.2 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, or technology being developed.

Specify whether the System collects personally identifiable information (PII) on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

- From whom is information to be collected?
Employers and their agents sponsoring foreign workers for permanent labor certifications.
- Why is the Information being collected?
The information is collected to enable the processing of permanent worker applications.
- What is the PII being collected, used, disseminated, or maintained?
PII collected includes non-citizen (applicant) names, dates of birth, addresses, government-issued identifiers, personal phone numbers, work experience and educational / work / training records.
- How is the PII collected?
Employers seeking to sponsor foreign workers for permanent visas use the system for online submission of permanent labor certification applications to DOL.
- How will the information collected from individuals or derived from the system be checked for accuracy?
The information is not checked for accuracy because that is not required.
- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?
 - Immigration and Nationality Act, as amended, 8 U.S.C. 1101(a)(15)(H)(i), and (ii), 1184(c), 1182(m) and (n), 1182(a)(5)(a), 1188, and 1288. Section 122 of Pub. L. 101 - 649. 8 CFR 214.2(h). 20 CFR 655 Subpart A. 20 CFR 655.9; and
 - Privacy Act of 1974
- Privacy Impact Analysis
A PIA is conducted because the system processes and stores sensitive PII of non-citizen applicants seeking permanent employment. DOL has implemented various security controls including SSL/TLS enabled websites to mitigate the risk of a data breach.

1.3 DESCRIBE THE USES OF THE PII

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

- Describe all the uses of the PII
The information is used to determine the eligibility of the applicants for a given visa category.
- What types of tools are used to analyze data and what type of data may be produced?
Not applicable. Tools are not used to analyze the data.
- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
FLCS-FLAG does not derive new data through aggregation of collected information.
- If the system uses commercial or publicly available data, please explain why and how it is used.
FLCS-FLAG does not use commercial or publicly available data.
- Will the use of PII create or modify a “system of records notification” under the Privacy Act?

The System of Records Notice (SORN) below has been published for the system (See ETA Standard SORN - <https://www.dol.gov/agencies/sol/privacy/eta-7>).

○ DOL/ETA – 7 Employer Application and Attestation file for Permanent and Temporary Alien Workers

- Privacy Impact Analysis

DOL has implemented various security controls to protect the data to include:

- Enabling SSL/TLS on websites for collection of data;
- Encrypting sensitive data at-rest;
- Enabling access controls including account management, monthly access reviews (semi-annual user recertification and separated users review), monthly access log reviews, access enforcement, and account lock mechanisms
- Enabling audit monitoring, logging, analysis, and reporting
- Deploying F5 application (network) firewalls to protect application systems;
- Conducting application vulnerability scans, annual security assessments and remediating findings;
- Conducting Security Impact Assessments prior to deploying code to Production

1.4 RETENTION

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

- What is the retention period for the data in the system?

For FLAG, Records are maintained within the system indefinitely.

- Is a retention period established to minimize privacy risk?

No

Has the retention schedule been approved National Archives and Records Administration (NARA)?

No, ETA OFLC are activity working on revising record retention schedules and obtaining approval with NARA.

- Per *M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored, or maintained by the system if it is no longer required?

OFLC Case Files are retained indefinitely. Paper files are retained on-site at national processing centers for six months from the date of final determination. OFLC will continuously scan or convert paper records into OFLC Archive and Scan database(s). Paper copies of employer applications that are scanned will be destroyed once converted to an electronic medium and verified, or when no longer needed for legal or audit purposes in accordance with the records schedule for a period of 5 years.

- How is it determined that PII is no longer required?

Records are maintained within the system indefinitely.

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

The FLAG systems are not allowed to eliminate PII from the system.
The PII reside on the system indefinitely.

- Privacy Impact Analysis

Risk are minimum as DOL encrypts sensitive data in the databases and keeps an audit trail of attempts to access and decrypt the data.

1.5 INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

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

PII is shared with the Wage and Hour Division and OIG as required for investigations.

- How is the PII transmitted or disclosed?

PII is disclosed through system access to authorized users.

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

Yes. There is a continuous need for information during investigations. Accounts that are not utilized in 60 days are deactivated.

- Privacy Impact Analysis

Risks are minimum as the system enable automatic account management and access to data are disclosed to authorized users.

1.6 EXTERNAL SHARING AND DISCLOSURE

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

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

Data is shared with DHS USCIS for the purpose of business existence verification. The Form ETA-9089 data fields are shared through OCIO's Data as a Service secured connection between DOL and DHS.

- Is the sharing of PII 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 PII outside of DOL.

Yes. The DHS Systems of Records (SORN) used for purposes of this information exchange are:

1. DHS/USCIS-007 - United States Citizenship and Immigration Services Benefits Information System, September 29, 2008, 73 FR 56596.
2. DHS/USCIS-014 - Electronic Immigration System-I Temporary Accounts and Draft Benefit Requests System of Records, April 5, 2013, 78 FR 20680.
3. DHS/USCIS-015 - Electronic Immigration System-2 Account and Case Management System of Records, April 5, 2013, 78 FR 20673.
4. DHS/USCIS-016 - Electronic Immigration System-3 Automated Background Functions System of Records, November 15, 2011, 76 FR 70735.
5. DHS/NPPD-001 -Arrival and Departure Information System, May 28, 2013, 78 FR 31955.

The DOL System of Records (SORN) used for purposes of this information exchange is the DOL/ETA-7 - Foreign Labor Certification System and Employer Application Case Files.

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

Data is shared through OCIO's Data as a Service secured connection between DOL OFLC Systems and DHS USCIS' Validation Instrument for Business Enterprises (VIBE) system.

- o All traffic is routed through a DHS Secure VPN Tunnel
- o Access to the DOL DaaS service is controlled with a "White-List" of allowed IP addresses
- o An assigned API Key is required to run the DOL DaaS service
- o Connection Protocol is Transport Layer Security (TLS) v1.2
- o FLAG uses Datahub, a data sharing platform to share application data and documents
- o Datahub is periodically scanned for infrastructure and system level vulnerabilities on

both the OS images and libraries in-use / adopted with discovered vulnerabilities tracked / monitored to full resolution

- How is the information transmitted or disclosed?

The VIBE system makes requests for data to the DOL DaaS service on a near real-time case by case basis. The DOL DaaS service responds with a JSON formatted message containing updated case data. The amount of case data varies depending on the DOL workload.

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? **If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.**

An MOU with the Department of Homeland Security was finalized on February 2021. OFLC provides information submitted by employers through the Program Electronic Review Management (PERM) system to DHS/USCIS.

The MOUs will enable FLCS-FLAG to share information with Department of Justice and Department of State.

- How is the shared information secured by the recipient?

Shared information is secured by Internet Protocol Security (IPSec) Advanced Encryption Standard-256 (AES-256) encrypted tunnels.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

USCIS and DOL, including all personnel with access to the information, will be appropriately trained regarding the proper handling of PII and proper care of the information systems to ensure the overall safeguarding and security of the information. USCIS and DOL will cross-train to ensure that each agency's employees, including contractors with access to any of the information, have completed privacy training on the handling of PII, which includes information on applicable laws, regulations, and policies related to information privacy and security, as well as on immigration-specific confidentiality protections as required.

- Privacy Impact Analysis

Risks are minimal due to strong in-transit encryption adopted for data transfers (AES-256 via IPSec Tunnels) with IP whitelisting enabled along with pre-assigned API keys required and strict user authorization enforced for access.

1.7 NOTICE

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

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.

The System of Records Notice (SORN) below has been published for the system (See ETA Standard SORN - <https://www.dol.gov/agencies/sol/privacy/eta-7>).

- DOL/ETA – 7 Employer Application and Attestation file for Permanent and Temporary Alien Workers

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

Individuals can withdraw from the program.

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

No

- Privacy Impact Analysis

Individuals voluntarily provide their information and have the option of withdrawing from the program.

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

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

- What are the procedures that allow individuals to gain access to their own information?

Each application for a labor certification is identified by a case number and access to data on that case is restricted to users with account access. The foreign labor worker will obtain their formation from their respective employer.

- What are the procedures for correcting inaccurate or erroneous information?

Users with access to the case, must withdraw the inaccurate application and submit a corrected application.

- How are individuals notified of the procedures for correcting their own information?

Individuals are notified through constructive notice given via the published SORN for FLAG (See ETA Standard SORN - <https://www.dol.gov/agencies/sol/privacy/eta-7>). Filers also sign an attestation that the information is accurate at the time of submission. DOL relies on the attestation.

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

Not applicable

- Privacy Impact Analysis

Applicants have the right to withdraw from the program.

1.9 TECHNICAL ACCESS AND SECURITY

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

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Program managers, IT Specialists, Analysts, and registered Users with limited access to their data.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA.

External contractors (Booz-Allen Hamilton) who maintain the system does have access to the system. Riva Solutions contractors who support the reviewing of foreign applications.

- Does the system use “roles” to assign privileges to users of the system? If yes, describe the roles.

Yes; there are different privileges for external users, data entry clerks, case processing analysts, center directors/certifying officers, and system administrators for FLAG. External users may submit cases and review case statuses. Data entry clerks enter applications that were received by mail at the national processing centers (NPCs). Case processing analysts review cases and recommend decisions. Center directors or certifying officers review the recommendations and issue certifications or denials. System administrators assign user permissions based on access request forms and perform account maintenance tasks such as password resets or changes of email address.

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

Yes. OCIO has developed the FLCS-FLAG Access Request form, which documents the level of access and/or privileges assigned each user.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided? Provide date of last training.

DOL provides Security Awareness training, at least annually, via LearningLink. The last training was provided in May 2022.

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

DOL Privacy Security Awareness training.

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

DOL keeps an audit trail of all attempts to access data in the databases. RBAC to manage access to read and write data at the application level. DOL monitor audit logs to monitor user actions and detect data misuse.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

Yes. the last Security Assessment was performed in August 2021 and the system was last authorized to operate until June 2023.

- Privacy Impact Analysis

The privacy risks identified include data loss or inadvertent disclosure and misuse of PII data information. DOL mitigates these risks by implementing adequate access controls, deploying solid encryption, and assigning users with least privileges.

1.10 TECHNOLOGY

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

- Was the system built from the ground up or purchased and installed?

The system was built from the ground up.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.

DOL conducts annual/ad hoc security assessments (including PIAs) of the system.

- What design choices were made to enhance privacy?

DOL encrypts FLCS-FLAG data in transit and at rest and provides users with limited privileges commensurate with their job functions/roles.

- For systems in development, what stage of development is the system in, and what project development life cycle was used?

FLCS-FLAG is operational; the system development conforms to the computer security lifecycle defined in DOL System Development Lifecycle Management Manual (SDLCMM). Based on the criteria in the SDLCMM, the system is in the 'Operations and Maintenance' phase.

- For systems in development, does the project employ technology which may raise privacy concerns? If so please discuss their implementation?

FLCS-FLAG does not employ technologies that may raise privacy concerns.

1.11 DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

DOL OCIO has completed the PIA for FLCS-FLAG which is currently in operation. DOL OCIO has determined that the safeguards and controls for this moderate system adequately protect the information.

DOL OFLC has determined that it is collecting the minimum necessary information for the proper performance of a documented agency function.

1.12 PIA SIGNATURE PAGE

Responsible Officials

Signature of System Owner

Signature of ETA OFLC

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained?
Also, note whether the collection is for ☐ Federal employees, ☐ Contractor staff, ☒ Members of the Public {Check all that apply}

- ☒ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr.
- ☒ First name ☒ Middle initial and/or ☒ Last
- ☒ Name suffix such as Jr. Sr., etc.
- ☒ Date of birth
- ☒ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☒ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license plate, VIN)
- ☐ Driver's license number
- ☒ Residential address
- ☐ Personal phone numbers (e.g., phone, fax, cell)
- ☒ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address
- ☒ Business address

- ☒ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☒ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☒ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☐ Digital signing or encryption certificate
- ☒ Other: Case No.
- ☐ None

- Is any part of the PII collection voluntary?

Applicants can withdraw from the program.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

Not applicable; FLCs does not store nor process SSNs.

APPENDIX B : FLCS FLAG SYSTEM TRACKING TEMPLATE

Program/System:

OCIO FLCS FLAG supporting ETA FLC

Purpose and Use:

FLCS-FLAG enables the Department to meet statutory and regulatory provisions requiring all employers seeking a labor certification for either permanent or temporary nonimmigrant labor to apply through the OFLC. The programs and services currently administered by the OFLC includes:

- The immigrant Permanent Labor Certification Program (PERM) or the “Green Card”;
- The nonimmigrant H-1B and H-1B1 (Chile and Singapore) Specialty Occupations Programs;
- E-3 Specialty Worker Program (Australia); H-2A Temporary Agricultural Program;
- H-2B Temporary Non-agricultural Program;
- CW-1 Commonwealth of the Northern Mariana Island Workers (CNMI); and
- The D-1 Longshore Crewmember Program.

FLCS-FLAG enables OFLC to achieve planned application modernization goals that include:

- Enhanced user experience: Improvements to customer filing experience using a central web interface with single sign-on, automated login/user security management, and mobile application design;
- Custom configuration: Lack of adequate personalization of user accounts, automated alerts, and customer relations management (i.e., Government-to-Business correspondence) on applications;
- Better capabilities: Enhanced forms preparation, helpful tips, e-checks, automated field population, and digital signature and document management capabilities;
- Workflow approach: More robust application assignment and workflow capabilities with customizable adjudication review processes and procedures;
- Intuitive interface: Enhanced application search functions, document management capabilities, and customizable correspondence templates and content to promote more streamlined application processing for internal users;
- Reports and dashboards: Enhanced operational reporting, data analytics, and data visualization capabilities;
- Help desk: Enter, track, and resolve customer inquiries (i.e., Help Desk) in a timely manner.
- Smart decisions: Automate and streamline workflow processes and improve overall efficiency, quality, and consistency of decision-making.

The FLCS supports the Strategic Goal 1 – Prepare workers for good jobs & ensure fair compensation. Foreign workers may be legally hired on a temporary or permanent basis when no American workers are available, able, willing and qualified, provided their employers file applications with the Department to adequately document the need.

Legal Authority:

Immigration and Nationality Act, as amended, 8 U.S.C. 1101(a)(15)(H)(i), and (ii), 1184(c), 1182(m) and (n), 1182(a)(5)(a), 1188, and 1288. Section 122 of Public Law 101-649. 8 CFR 214.2(h). 20 CFR 655 Subpart A. 20 CFR 655.9.

System Access:

1. USCIS and DOL/ETA government and contracted employees
2. Employees or contract employees of other DHS Components and other Federal agencies
3. Employees or contract employees of other USDA Components and other Federal agencies

Individuals Impacted:

Foreign members of the public, business employers, agents and attorneys who file requests for permanent labor certification.

Source s of Information:

The records are entered and maintained through the end user web browser to DOL web application, data is contained within labor certification, and labor condition application databases.

Data Elements:

Employers' names, addresses, type and size of businesses to include annual gross revenue and proof of insurance coverage, production data, number of workers needed in certain cases, offer of employment terms to known or unknown aliens, and background and qualifications of certain aliens, along with resumes and applications of U.S. workers, employer provided source wage documents and surveys, agent/attorney names and addresses, agent/attorney business details, Foreign applicates PII. In addition to PII data, the system also collects application and temporary need information, Employer and Point of Contact Information, H-2A labor contractor information, declaration and application prepare information, case status, processing events, and related case management information.

SORN Coverage:

DOL/ETA-7, Foreign Labor Certification System and Employer Application Case Files

Records Retention Period:

Records are maintained within the system indefinitely.