



[Home](#) > [Policy Manual](#)

Chapter 7 - Privacy and Confidentiality

Guidance

[Resources \(27\)](#)

[Appendices \(0\)](#)

[Updates \(6\)](#)

[History \(0\)](#)

A. Privacy Act of 1974

The Privacy Act provides that federal agencies must protect against the unauthorized disclosure of personally identifiable information (PII) that it collects, disseminates, uses, or maintains.^[1] The Privacy Act requires that personal information belonging to U.S. citizens and lawful permanent residents (LPRs) be protected from unauthorized disclosure. Violations of these requirements may result in civil and criminal penalties.

B. Fair Information Practice Principles

DHS treats all persons, regardless of immigration status, consistent with the Fair Information Practice Principles (FIPPs).^[2] The FIPPs are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974. The principles are:

- Transparency;
- Individual participation;
- Purpose specification;
- Data minimization;
- Use limitation;
- Data quality and integrity;
- Security; and
- Accountability and auditing.

The table below provides a description of each principle.

Fair Information Practice Principles

DHS Framework for Privacy Policy

| Principle | Description |
|------------------------------------|--|
| <i>Transparency</i> | DHS provides transparency for how it handles sensitive information through various mechanisms, including Privacy Impact Assessments, System of Records Notices, Privacy Act Statements, and the Freedom of Information Act (FOIA). |
| <i>Individual Participation</i> | To the extent practicable, DHS should involve persons in the process of using their personal information, and they may always request information about themselves through a FOIA request. |
| <i>Purpose Specification</i> | DHS' default action should be to not collect information, and if it is otherwise necessary, DHS should articulate the authorities that permit collection and must clearly state the purposes of the information collection. |
| <i>Data Minimization</i> | DHS collects only information relevant and necessary to accomplish the purposes specified and special emphasis is placed on reducing the use of sensitive personal information, where practical. |
| <i>Use Limitation</i> | Any sharing of information outside of the agency must be consistent with the use or purpose originally specified. |
| <i>Data Quality and Integrity</i> | DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete. |
| <i>Security</i> | DHS uses appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification or unintended or inappropriate disclosure. |
| <i>Accountability and Auditing</i> | DHS has a number of accountability mechanisms, including reviews of its operations, training for employees, and investigations when appropriate. |

C. Personally Identifiable Information

DHS defines PII as any information that permits the identity of a person to be directly or indirectly inferred, including any information which is linked or linkable to that person regardless of whether the

person is a U.S. citizen, lawful permanent resident (LPR), visitor to the United States, or a DHS employee or contractor.^[3]

Sensitive PII is defined as information which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to a person.^[4] Some examples of PII that USCIS personnel may encounter include:

- Name;
- Address;
- Date of birth; and
- Certificate of Naturalization or Citizenship number.
- Alien number (A-number);
- Social Security number;
- Driver's license or state ID number;
- Passport number; and
- Biometric identifiers.

USCIS employees have a professional and legal responsibility to protect the PII the agency collects, disseminates, uses, or maintains. All USCIS employees must follow proper procedures when handling all PII and all information encountered in the course of their work. All USCIS employees processing PII must know and follow the policies and procedures for collecting, storing, handling, and sharing PII. Specifically, USCIS employees must:

- Collect PII only when authorized;
- Limit the access and use of PII;
- Secure PII when not in use;
- Share PII, only as authorized, with persons who have a need to know; and
- Complete and remain current with all privacy, computer security, and special protected class training mandates.

D. Case-Specific Inquiries

USCIS receives a variety of case-specific inquiries, including requests for case status updates, accommodations at interviews, appointment rescheduling, and the resolution of other administrative issues. USCIS personnel are permitted to respond to these inquiries if:

- The requestor is entitled to receive the requested case-specific information; and
- Disclosure of the requested case-specific information would not violate Privacy Act requirements or other special protected class confidentiality protections.

1. Verifying Identity of Requestor

USCIS employees must verify the identity of a person inquiring about a specific application or petition. For in-person inquiries, those present must provide a government-issued identity document so that USCIS can verify their identity.

For inquiries not received in person (for example, those received through telephone call or email), it may be difficult to verify the identity of the person making the request through a government-issued document. In these cases, USCIS employees should ask for specific identifying information about the case to ensure that it is appropriate to communicate case-specific information. Examples of identifying information include, but are not limited to: receipt numbers, A-numbers, full names, dates of birth, email addresses, and physical addresses.

If a person is unable to provide identifying information that an applicant, petitioner, or representative should reasonably know, USCIS employees may refuse to respond to the request, or direct the requestor to make an appointment at a local field office or create a myUSCIS account.

2. Disclosure of Information

Except for case types with heightened privacy concerns,^[5] USCIS employees may communicate about administrative case matters if the requestor is able to demonstrate his or her identity (for example, by showing government-issued identification during an in-person encounter), or provide verifying information sufficient to demonstrate that communication would be proper. Administrative case matters are generally any issues that do not involve the legal substance or merit of an application or petition.

USCIS employees should not disclose PII when responding to case-specific requests; inquiries can generally be resolved without any discussion of PII.^[6] To ensure that a USCIS employee is not disclosing PII, the USCIS employee can always require that the requestor first provide and confirm any PII at issue. In addition, a USCIS employee may take action that results in the resending of cards, notices, or documents containing PII to addresses on file instead of directly disclosing PII to a requestor.

Interested parties may be present at in-person appointments or during telephone calls, with the consent of the applicant or petitioner. Consent is usually implied if both the applicant or petitioner and the third party are present together. However, a USCIS employee may always ask the applicant or petitioner if he or she consents to the third-party's presence if there is any doubt.

3. Communication with Address on File

USCIS sends written responses and duplicate notices to the addresses on file. Before USCIS is able to send any correspondence to a different address, the person must initiate a service request to update his or her address in USCIS systems.^[7] Change of address requests associated with cases subject to confidentiality provisions must follow separate procedures.^[8]

4. Third-Party Information

Information from other agencies, such as Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), or the Department of State (DOS) may be located in USCIS files and systems. This

information must not be released in response to an inquiry, although it may be appropriate to refer the inquiry to another agency.

5. Third-Party Government Inquiries

USCIS may share records covered under the Privacy Act with written consent from the person or pursuant to a routine use listed in the applicable [System of Records Notices](#). Before sharing information with a government entity, USCIS must determine if the disclosure and use of information is compatible with an existing routine use. Planned uses must also be compatible with the purpose for which DHS originally collected the information. There are, however, enumerated exceptions of the Act that may apply.

Congress

One exception is for disclosures to either house of Congress, or any Congressional committee, subcommittee, joint committee, or subcommittee of a joint committee, if the matter is within its jurisdiction. For all other requests from members of Congress, such as constituent requests, the person whose information is to be released must have provided the member of Congress with a privacy release for USCIS to disclose any information related to that person.

The USCIS Office of Legislative and Intergovernmental Affairs (OLIA) and designated liaisons handle all inquiries and certain correspondence from Congress to USCIS. Members of Congress, congressional offices, and congressional committees should always go through OLIA when initiating an inquiry. The [USCIS and Congress](#) webpage on USCIS' website provides instructions on how members of Congress should interact with and [contact USCIS](#). Non-liaison USCIS employees who are contacted directly with a congressional inquiry should refer it to OLIA so that it may proceed through the proper channels.

Law Enforcement Agencies

Information may be shared with other DHS components under the existing DHS information sharing policy,^[9] which considers all DHS components one agency, as long as there is a mission need in line with the requestor's official duties.

Requests from law enforcement agencies outside of DHS must go through [DHS Single Point of Service \(SPS\) Request for Information \(RFI\) Management Tool](#), which requires an account. Account requests can be submitted to DHS-SPS-RFI@hq.dhs.gov.

Before referring any relevant RFI to USCIS, SPS ensures any RFI is consistent with the USCIS mission, has been reviewed and cleared by DHS Counsel and Privacy (as required), and is provided a tracking number. SPS then submits the RFI to Fraud Detection and National Security (FDNS) Intelligence Division (ID). FDNS ID logs official RFIs and takes the necessary steps to process and answer them, including review by USCIS Office of Chief Counsel and Office of Privacy.

Federal Investigators

If an Office of Personnel Management or DHS Office of Inspector General (OIG) investigator requests information, the USCIS employee should provide the information upon verifying the requestor's identity. Disclosure of any information needs to meet a routine use or be covered by a data share agreement. USCIS employees and contractors must provide prompt access for auditors, inspectors, investigators, and other personnel authorized by the OIG to any files, records, reports, or other information that may be requested either orally or in writing, and supervisors may not impede this cooperation.

Other Third-Party Inquiries

Prior to responding to a non-congressional third-party case inquiry, a written, signed, and notarized privacy release must be obtained from the applicant or petitioner. Third parties should submit a written authorization and identify the information the person desires to be disclosed. USCIS staff can accept the authorization via facsimile or email as long as the signature on the original is handwritten, and not typed or stamped.^[10] The USCIS Office of Privacy will conduct an analysis for disclosure requests for PII on persons not covered by the Privacy Act or the Judicial Redress Act, absent another mechanism that confers a right or process by which a member of the public may access agency records.

E. VAWA, T, and U Cases

1. Confidentiality Provisions

Applicants and recipients of immigration relief under the Violence Against Women Act of 1994 (VAWA)^[11] and the Victims of Trafficking and Violence Prevention Act of 2000^[12] (T and U nonimmigrant status for victims of trafficking and other serious crimes) are entitled to special protections with regard to privacy and confidentiality. The governing statute prohibits the unauthorized disclosure of information about petitioners and applicants for, and beneficiaries of VAWA, T, and U-related benefit requests to anyone other than an officer or employee of DHS, the Department of Justice (DOJ), or the Department of State (DOS) who has a need to know.^[13]

This confidentiality provision is commonly referred to as “Section 384” because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996,^[14] which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief.

An unauthorized disclosure of information which relates to a protected person can have significant consequences. USCIS employees must maintain confidentiality in these cases. Victims of domestic violence, victims of trafficking, and victims of crimes can be put at risk, as can their family members, if information is provided to a person who is not authorized.

Anyone who willfully uses, publishes, or permits any information pertaining to such victims to be disclosed in violation of the above-referenced confidentiality provisions may face disciplinary action and be subject to a civil penalty of up to \$5,000 for each violation.

2. Scope of Confidentiality

Duration of Confidentiality Requirement

By law, the confidentiality provisions apply while a VAWA, T, or U case is pending and after it is approved, and ends when the application for immigration relief is denied and all opportunities for appeal of the denial have been exhausted.

Disclosure of Information

USCIS cannot release any information relating to a protected person until the identity of the requestor of information is verified and that person’s authorization to know or receive the protected information is

verified. Such identity and eligibility verification must be done before responding to any inquiry, expedite request, referral, or other correspondence. Upon identity verification, USCIS can provide protected information directly to the protected person or his or her representative authorized to receive 1367-protected information.

Exceptions for Disclosure of Information

USCIS is permitted to disclose information relating to a protected person in certain, limited circumstances. These circumstances include:

- Statistical Information – Disclosure of data and statistical information may be made in the manner and circumstances permitted by law.^[15]
- Legitimate Law Enforcement Purposes – Disclosure of information may be made to law enforcement officials to be used solely for a legitimate law enforcement purpose.
- Judicial Review – Information can be disclosed in connection with judicial review of a determination provided it is in a manner that protects the confidentiality of the information.
- Applicant Waives Confidentiality – Adults can voluntarily waive the confidentiality provision; if there are multiple victims in one case, they must all waive the restrictions.
- Public Benefits – Information may be disclosed to federal, state, and local public and private agencies providing benefits, to be used solely in making determinations of eligibility for benefits.^[16]
- Congressional Oversight Authority (for example, Government Accountability Office audits) – The Attorney General and the Secretary of Homeland Security can disclose information on closed cases to the chairmen and ranking members of Congressional Committees on the Judiciary, for the exercise of Congressional oversight authority. The disclosure must be in a manner that protects the confidentiality of the information and omits PII (including location-related information about a specific person).
- Communication with Non-Governmental Organizations (NGO) – Government entities adjudicating applications for relief^[17] and government personnel carrying out mandated duties under the Immigration and Nationality Act (INA)^[18] may, with the prior written consent of the person involved, communicate with nonprofit NGO victims' service providers for the sole purpose of assisting victims in obtaining victim services. Agencies receiving referrals are bound by the confidentiality provisions.
- National Security Purposes – The Secretary of Homeland Security, the Secretary of State, or the Attorney General may provide in their discretion the disclosure of information to national security officials to be used solely for a national security purpose in a manner that protects the confidentiality of such information.
- To sworn officers or employees of the Department of State or Department of Justice, for legitimate Department, bureau, or agency purposes.

3. USCIS Assistance

USCIS employees must ensure confidentiality is maintained when an applicant, petitioner, or beneficiary of certain victim-based benefits requests assistance.

Change of Address

Applicants with VAWA, T, or U-related cases can request a change of address by submitting an Alien's Change of Address Card ([Form AR-11](#)) with an original signature to the Vermont Service Center (VSC) by mail.

If the requestor previously filed for a waiver of the I-751 joint filing requirement because of abuse, the requestor should file a [Form AR-11](#) with an original signature with the USCIS office assigned to work the Form I-751. The requestor can find the appropriate USCIS office by referring to the receipt number issued in response to the Form I-751 filing. [\[19\]](#)

An applicant may also appear in person at a USCIS field office to request a change of address, by calling the USCIS Contact Center at 1-800-375-5283 (TTY: 1-800-767-1833) to request an in-person appointment. The applicant's identity must be verified before making the requested change. If the case is at the VSC or the Nebraska Service Center (NSC), the field office must also notify the VSC or NSC of the change of address for VAWA, T, and U cases.

Telephonic Inquiries

The identity of the person inquiring about a confidential case must be verified and that person's eligibility to receive information must also be verified. Such verification cannot be made telephonically.

F. Asylees and Refugees

1. Confidentiality Provisions

Federal regulations generally prohibit the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations. [\[20\]](#) This includes information contained in the legacy Refugee Asylum and Parole System (RAPS) or the legacy Asylum Pre-Screening System (APSS), and Global System (the 2018 replacement for RAPS/APSS) or related information as displayed in CIS2 and PCQS, except under certain limited circumstances. As a matter of policy, the confidentiality protections in these regulations are extended to Registration for Classification as Refugee (Form I-590), Refugee/Asylee Relative Petitions ([Form I-730](#)), and Applications for Suspension of Deportation or Special Rule Cancellation pursuant to NACARA ([Form I-881](#)).

These regulations safeguard information that, if disclosed publicly, could subject the claimant to retaliatory measures by government authorities or non-state actors in the event the claimant is repatriated. Such disclosure could also endanger the security of the claimant's family members who may still be residing in the country of origin.

Moreover, public disclosure might give rise to a plausible protection claim by the claimant where one would not otherwise exist. This is because such disclosure may bring an otherwise ineligible claimant to the attention of the government authority or non-state actor against which the claimant has made allegations of mistreatment.

2. Breach of Confidentiality

Confidentiality is breached when the unauthorized disclosure of information contained in or pertaining to, these protected classes allows the third party to link the identity of the applicant to:

- The fact that the applicant or petitioner has applied for asylum or refugee status;
- Specific facts or allegations pertaining to the individual asylum or refugee claim contained in an asylum or refugee application; or
- Facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum or refugee status.

The same principles generally govern the disclosure of information related to credible fear and reasonable fear determinations, and applications for withholding or deferral of removal under Article 3 of the Convention Against Torture, which are encompassed within the Application for Asylum and for Withholding of Removal (Form I-589). As a matter of policy, USCIS extends the regulatory safeguards to include claims under the Safe Third Country Agreement, applications for suspension of deportation, special rule cancellation of removal under NACARA 203, refugee case information, as well as refugee and asylee relative information.

Disclosures may only be made to U.S. government officials or employees and U.S. federal or state courts where there is a demonstrated need-to-know related to certain administrative, law enforcement, and civil actions. Any other disclosure requires the written consent of the claimant or the express permission of the Secretary of DHS.

3. USCIS Assistance

USCIS employees must not disclose information contained in, or pertaining to, any asylum or refugee application or claim to any third party without the written consent of the applicant, except as permitted by regulation or at the discretion of the Secretary of DHS. [\[21\]](#)

This includes neither confirming nor denying that a particular person filed a protection claim by submitting any of the following:

- An Application for Asylum and for Withholding of Removal ([Form I-589](#));
- A Registration for Classification as Refugee (Form I-590);
- A Refugee/Asylee Relative Petition (Form I-730);
- A Request for a Safe Third Country Agreement Determination;
- A Request for a Credible Fear Determination;
- A Request for a Reasonable Fear Determination; and
- An Application for Suspension of Deportation or Special Rule Cancellation of Removal (Pursuant to Section 203 of Public Law 105-100 (NACARA) (Form I-881)).

USCIS employees should respond to inquiries related to Form I-589, Form I-881, requests for information pertaining to the Safe Third Country Agreement, credible fear and reasonable fear processes, Form I-590, and Form I-730 in different ways, depending on the inquiry:

Request for Disability Accommodation at an Upcoming Form I-589 Interview

Tier 2 staff members may use the Service Request Management Tool (SRMT) to record and transfer requests to the asylum office with jurisdiction over the pending application. The asylum office then contacts the applicant to arrange for disability accommodation at the interview. While officers must not confirm or deny the existence of a pending protection claim or NACARA 203 application, those making disability accommodation requests for upcoming asylum interviews should be told that the request is being recorded and will be forwarded to the appropriate office for follow-up.

Change of Address Request

Tier 2 staff members may create a service request and submit it to the asylum office or service center with jurisdiction over the pending Form I-589, Form I-881, or Form I-730 petition. The office then fulfills the service request. While staff members must not confirm or deny the existence of a pending protection claim, those making address change requests should be told that the request is being recorded and will be forwarded to the appropriate office.

USCIS Contact Center Status Inquiries for Form I-589, Form I-881, and Form I-730

USCIS Contact Center personnel may not respond to any status inquiries, and may not confirm or deny the existence of an application or petition. Instead, USCIS Contact Center personnel should direct the caller to the [Case Status Online](#) tool. If the caller needs further assistance than the Case Status Online tool can provide, USCIS Contact Center personnel should direct the caller to the local office with jurisdiction over the application. For information on office-specific in-person appointment requirement, see the [Asylum Office Locator](#) tool. The office with jurisdiction over the application must respond to the inquiry.

USCIS Contact Center Status Inquiries for Form I-590 Applications

USCIS Contact Center personnel may not respond to any status inquiries and may not confirm or deny the existence of an application or petition. Instead, USCIS Contact Center personnel should obtain all relevant information from the inquirer and refer the inquiry to the USCIS Headquarters International and Refugee Affairs Division (IRAD) for response.

Inquiries Regarding Subsequent Applications or Petitions Based on Underlying Form I-589, Form I-590, or Form I-730

Staff members may respond to inquiries regarding subsequent applications or petitions that are based on an underlying Form I-589, Form I-590, or Form I-730 (including Application for Travel Document ([Form I-131](#)), Application for Employment Authorization ([Form I-765](#)), or Application to Register Permanent Residence or Adjust Status ([Form I-485](#))). Staff members may not confirm or deny the existence of the underlying application.

General Inquiries

USCIS employees may respond to general questions about the asylum program, the U.S. Refugee Admission Program (USRAP), and credible and reasonable fear screenings.^[22] However, for all specific case status questions relating to I-589 applications or I-730 petitions, the inquirers must be directed to contact the local asylum office or service center with jurisdiction over the application. For specific case status questions relating to I-590 refugee applications, the inquiry must be referred to RAD for response.

Asylum offices may accept case inquiries from the applicant or the applicant's attorney or representative with a properly completed Notice of Entry of Appearance as Attorney or Accredited Representative ([Form G-28](#)) on file.

Asylum offices may receive case inquiries in a variety of ways, such as by mail, email, phone, fax, or in person. When it is possible to verify the identity of the applicant or attorney or representative inquiring, offices may respond using any of those communication channels. If it is not possible to verify the identity of the inquirer, asylum offices should respond to inquiries by providing a written response to the last address the applicant provided.

RAD does not respond to inquiries over the phone, but instead asks the inquirer to put his or her request in writing so that the signature and return address can be compared to information on file. RAD responds to an inquiry received by email only if the email address matches the information the applicant submitted to the Resettlement Support Center or if the principal applicant provides written consent that includes the principal applicant's signature.

G. Temporary Protected Status

1. Confidentiality Provisions

Like refugee and asylum cases, information pertaining to Temporary Protected Status (TPS) cases may not be disclosed to certain third parties because unauthorized disclosure of information may place the applicant or the applicant's family at risk.^[23]

The law prohibits the release of information contained in the TPS application or in supporting documentation to third parties without the written consent of the applicant. A third party is defined as anyone other than:

- The TPS applicant;
- The TPS applicant's attorney or authorized representative (with a properly completed Notice of Entry of Appearance as Attorney or Accredited Representative ([Form G-28](#)) on file);
- A DOJ officer, which has also been extended to include a DHS officer following the transfer of certain immigration functions from DOJ to DHS; or
- Any federal or state law enforcement agency.

2. USCIS Assistance

USCIS may not release any information contained in any TPS application and supporting documents in any form to any third party, without a court order or the written consent of the applicant.^[24] Status inquiries may not confirm or deny the existence of a TPS application, or whether a person has TPS, until the identity of the inquirer has been confirmed and it has been determined the inquirer is not a third party to whom information may not be released.

USCIS employees must adhere to these same TPS confidentiality provisions regarding the disclosure of information to third parties, even if the information is contained in a TPS-related form such as:

- The Application for Employment Authorization ([Form I-765](#)), which every TPS applicant must file;
- A TPS-related waiver requested on Application for Waiver of Grounds of Inadmissibility ([Form I-601](#));
or
- A TPS-related Application for Travel Document ([Form I-131](#)).

With respect to confidentiality, USCIS employees must treat these records as they do other TPS supporting documentation in the TPS application package.

USCIS employees may respond to general questions about the TPS program.^[25] However, for all case-specific questions relating to Form I-821 applications, USCIS employees must first confirm the identity of the person and his or her eligibility to receive such information.

Offices must not take or respond to inquiries about the status of a TPS application made by telephone, fax, or email because it is not possible to sufficiently verify the identity of the inquirer. Offices may accept written status requests signed by the applicant (or the applicant's attorney or representative with a properly completed Notice of Entry of Appearance as Attorney or Accredited Representative ([Form G-28](#)) on file).

3. Exceptions for Disclosure

Information about TPS applications and information contained in supporting documentation can be disclosed to third parties in two instances:

- When it is mandated by a court order; or
- With the written consent of the applicant.

Information about TPS cases can be disclosed to officers of DOJ, DHS, or any federal or state law enforcement agency since they are not considered third parties.^[26] Information disclosed under the requirements of the TPS confidentiality regulation may be used for immigration enforcement or in any criminal proceeding.

H. Legalization

1. Confidentiality Provisions

Statutory and regulatory provisions require confidentiality in legalization cases and Legal Immigration Family Equity (LIFE) Act legalization cases, prohibiting the publishing of any information that may be identified with a legalization applicant.^[27] The laws also do not permit anyone other than sworn officers and employees of DHS and DOJ to examine individual applications.

Information contained in the legalization application can only be used in the following circumstances:

- To make a determination on the legalization application;
- For criminal prosecution of false statements violations;^[28] or

- In preparation of certain reports to Congress.

A breach in confidentiality of legalization cases can result in a \$10,000 fine.^[29]

2. USCIS Assistance

Case-specific information may be provided to the applicant and the applicant's attorney or authorized representative (with a properly completed Notice of Entry of Appearance as Attorney or Accredited Representative ([Form G-28](#)) on file) after the inquirer's identity has been verified. No others are authorized to receive legalization information unless one of the enumerated exceptions to disclosure noted below applies.

3. Exceptions for Disclosure

USCIS is permitted to disclose information pertaining to legalization cases in certain, limited circumstances. These circumstances include:

Law Enforcement Purposes

USCIS is required to disclose information to a law enforcement entity in connection with a criminal investigation or prosecution, when that information is requested in writing.

Requested by an Official Coroner

USCIS is also required to disclose information to an official coroner for purposes of affirmatively identifying a deceased person (whether or not the person died as a result of a crime).

Statistical Information

Disclosure of data and statistical information may be made in the manner and circumstances permitted by law.^[30]

Available from Another Source

USCIS may disclose information furnished by an applicant in the legalization application, or any other information derived from the application, provided that it is available from another source (for example, another application or if the information is publicly available).

I. Special Agricultural Workers

1. Confidentiality Provisions

Material in A-files filed pursuant to the Special Agricultural Workers (SAW) program is protected by strict confidentiality provisions.^[31] The statute provides that the employee who knowingly uses, publishes, or permits information to be examined in violation of the confidentiality provisions may be fined not more than \$10,000.^[32]

In general, USCIS may not use information furnished by the SAW applicant for any purpose other than to make a determination on the application, for termination of temporary residence, or for enforcement actions relating to false statements in applications.^[33] The applicant may not waive the confidentiality provisions, which even survive the death of the applicant.

2. USCIS Assistance

In general, it is permissible for USCIS employees to disclose only that an applicant has applied for SAW and the outcome of the adjudication. Case information may be provided to the applicant and the applicant's attorney or authorized representative (with a properly completed Notice of Entry of Appearance as Attorney or Accredited Representative ([Form G-28](#)) on file) after the inquirer's identity has been verified. No other parties are authorized to receive SAW information, unless one of the enumerated exceptions to disclosure noted below applies.

3. Exceptions for Disclosure

It is appropriate for DHS and DOJ employees to have access to SAW material. The materials are subject to the above-mentioned penalties for unlawful use, publication, or release. USCIS is permitted to disclose information pertaining to SAW cases in certain, limited circumstances. These circumstances include:

Law Enforcement Purposes

USCIS is required to disclose information to a law enforcement entity in connection with a criminal investigation or prosecution, when that information is requested in writing.

Requested by an Official Coroner

USCIS is also required to disclose information to an official coroner for purposes of affirmatively identifying a deceased person (whether or not the person died as a result of a crime).

Criminal Convictions

Information concerning whether the SAW applicant has at any time been convicted of a crime may be used or released for immigration enforcement or law enforcement purposes.

J. S Nonimmigrant Visa Category

Nonimmigrants under the S visa category are noncitizen^[34] witnesses or informants. An S nonimmigrant is not readily identified in USCIS systems. However, if a USCIS employee discovers that an inquiry is from an S nonimmigrant or from someone who has applied for such status, the case must be handled carefully.

Inquiries regarding the following should come from a law enforcement entity:^[35]

- An Interagency Alien Witness and Informant Record ([Form I-854A](#));
- An Interagency Alien Witness and Informant Adjustment of Status ([Form I-854B](#)); and
- An Application for Employment Authorization ([Form I-765](#)) filed on the basis of being a principal nonimmigrant witness or informant in S classification.

If USCIS receives an inquiry regarding the status of a Form I-854 or a Form I-765 filed as an S nonimmigrant, the USCIS employee must neither confirm nor deny the existence of such applications and should inform the person that inquiries on these applications must be submitted through appropriate law enforcement channels.

Under no circumstances may USCIS employees ask questions about the S nonimmigrant's role in cooperating with law enforcement, the type of criminal activity for which the nonimmigrant is an informant or witness, or any specific information about the case in which the S nonimmigrant may be involved.

K. Witness Security Program

1. Program Participants

Participation in the Witness Security Program (commonly known as the Witness Protection Program) is not reflected in USCIS systems. Applicants in the Witness Security Program should not tell anyone, including USCIS employees, that they are participants in the program. A separate immigration file is created for a new identity of a participant in the program, and information from before and after the change in identity must be in separate files. However, one file will have documentation of a legal name change.

2. USCIS Assistance

If an applicant indicates that he or she is in the Witness Security Program, the applicant should be referred to the [U.S. Marshals Service](#).^[36] Also, under no circumstances should USCIS employees ask questions about why or how the applicant was placed in the Witness Security Program or any specific information about the case which resulted in the applicant being placed in the Witness Security Program.

Footnotes

[^ 1] See Privacy Act of 1974, [Pub. L. 93-579 \(PDF\)](#), 88 Stat. 1896 (December 31, 1974) (codified at [5 U.S.C. 552a \(PDF\)](#)).

[^ 2] See [DHS Privacy Policy Guidance Memorandum \(PDF\)](#), issued April 25, 2017.

[^ 3] See [Privacy Incident Handling Guidance \(PDF\)](#), DHS Instruction Guide 047-01-008, issued December 4, 2017.

[^ 4] See [Privacy Incident Handling Guidance \(PDF\)](#), DHS Instruction Guide 047-01-008, issued December 4, 2017.

[^ 5] The enhanced privacy protections and other confidentiality protections associated with certain applications and petitions mean that merely acknowledging the existence of a pending petition or application could violate statutory and regulatory requirements. As a result, when responding to inquiries about these types of cases, including Violence Against Women Act (VAWA), T, U, and asylum cases, USCIS employees should follow the policies in place for those specific benefits. For more information, see

Section E, VAWA, T, and U Cases [[1 USCIS-PM A.7\(E\)](#)] through Section K, Witness Security Program [[1 USCIS-PM A.7\(K\)](#)].

[[^6](#)] A case's status generally refers to its current posture in the adjudication process, which is dictated by the last action taken. For example, a case could be pending background checks, with an officer, awaiting response to a request for evidence (RFE), or with a decision issued on a given date.

[[^7](#)] See [USCIS Change of Address web portal](#). See Chapter 4, Service Request Management Tool, Section B, Responding to Service Requests [[1 USCIS-PM A.4\(B\)](#)].

[[^8](#)] See Section E, VAWA, T, and U Cases, Subsection 3, USCIS Assistance [[1 USCIS-PM A.7\(E\)\(3\)](#)].

[[^9](#)] See [The DHS Policy for Internal Information Exchange and Sharing](#).

[[^10](#)] For requests from federal, state, or local government agency representatives who want to review or want copies of documents from an A-file, USCIS employees should refer to USCIS records procedures regarding outside agency requests for USCIS files.

[[^11](#)] See [Pub. L. 103-322 \(PDF\)](#) (September 13, 1994).

[[^12](#)] See [Pub. L. 106-386 \(PDF\)](#) (October 28, 2000).

[[^13](#)] See [8 U.S.C. 1367](#).

[[^14](#)] See [Pub. L. 104-208](#), 110 Stat. 3009-546, 3009-652 (September 30, 1996).

[[^15](#)] See [13 U.S.C. 8](#).

[[^16](#)] See [8 U.S.C. 1641\(c\)](#).

[[^17](#)] This applies to application for relief under [8 U.S.C. 1367\(a\)\(2\)](#).

[[^18](#)] See [INA 101\(i\)\(1\)](#).

[[^19](#)] For more information regarding change of address procedures, see the [Change of Address Information](#) webpage.

[[^20](#)] See [8 CFR 208.6](#).

[[^21](#)] See [8 CFR 208.6](#).

[[^22](#)] Examples of general inquiries include: who can apply for asylum or refugee status, how to apply for asylum or access the USRAP, bars to protection, whether applicants are eligible for work authorization, and number of days it normally takes before an interview is scheduled.

[[^23](#)] See [INA 244\(c\)\(6\)](#). See [8 CFR 244.16](#).

[[^24](#)] See [8 CFR 244.16](#) for exceptions.

[[^25](#)] Examples of general inquiries include: Who can apply for TPS, how to apply for TPS, bars to TPS, whether applicants are eligible for work authorization, and the number of days it normally takes to adjudicate an application for TPS.

[^ 26] See [8 CFR 244.16](#).

[^ 27] See [INA 245A\(c\)\(4\)-\(5\)](#) . See [8 CFR 245a.2\(t\)](#), [8 CFR 245a.3\(n\)](#) , and [8 CFR 245a.21](#).

[^ 28] See [INA 245A\(c\)\(6\)](#).

[^ 29] See [INA 245A\(c\)\(5\)\(E\)](#).

[^ 30] See [13 U.S.C. 8](#).

[^ 31] See [INA 210](#) . This pertains to the 1987-1988 SAW program.

[^ 32] See [INA 210\(b\)\(6\)\(D\)](#).

[^ 33] See [INA 210\(b\)\(7\)](#).

[^ 34] In this Policy Manual, the term noncitizen, unless otherwise specified, means a person who is not a citizen or national of the United States. This term is synonymous with “alien” as defined in INA 101(a)(3) ([8 U.S.C. 1101\(a\)\(3\)](#)).

[^ 35] See [8 CFR 274a.12\(c\)\(21\)](#).

[^ 36] Officers can find information on how to contact their local U.S. Marshals Service office (if they are in the United States) on the U.S. Marshals Service [website](#). Officers should advise applicants to consult with the U.S. Marshals Service on how to handle the disclosure of their participation in the Witness Protection Program.

Current as of March 23, 2022
