Privacy Impact Assessment
for the

Biometric Storage System

March 28, 2007

Contact Point
Elizabeth Gaffin
USCIS Privacy Officer
United States Citizenship and Immigration Services
202-272-1400

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The United States Citizenship and Immigration Services (USCIS) is developing the Biometric Storage System (BSS) to help streamline the established USCIS biometric and card production processes and become the centralized repository for all USCIS customer biometrics. BSS will route, store, and process 10-print[1] fingerprint biometrics and associated biographic information for biometric-based background checks on those individuals applying/petitioning for immigration benefits. BSS is a new system being developed incrementally and will replace the Image Storage and Retrieval System (ISRS). BSS will also replace aspects of the Benefit Biometric Support System (BBSS), while adding new functionalities that did not previously exist in either ISRS or BBSS.

Introduction

Implemented as a part of a USCIS enterprise-wide "Transformation Program," BSS will help transition the agency's data management practices to a paperless, more centralized, and unique identity driven methodology. BSS will become the centralized repository for all biometric data captured by USCIS from applicants filing immigration applications.

BSS is being developed and deployed to perform the following four roles: (1) to replace the ISRS and aspects of the BBSS; (2) to serve as the centralized repository of biometrics captured by USCIS used for biometric based background checks; (3) to serve as the centralized source of image sets for benefit card and document production; and (4) to facilitate biometric-based identity verification.

In its first role, BSS will replace ISRS and aspects of BBSS. ISRS data will be migrated to BSS and the ISRS system will be retired. ISRS is a legacy system that stores a limited amount of information related to 10-print fingerprints and card production information. BBSS is a legacy system that serves as the conduit from USCIS to the Federal Bureau of Investigation (FBI) for conducting fingerprint biometric background checks and storing the results. BSS will replace segments of BBSS by utilizing established direct links to the FBI and establishing new links to the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. This will make the process of sending 10-print biometrics to the FBI and US-VISIT more efficient by directly connecting to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) network and to US-VISIT's Automated Biometric Identification System database (US-VISIT/IDENT). BSS will assume all of ISRS's functionality and limited aspects of BBSS's functionality in the established USCIS processes.

In its second role, BSS will become the centralized repository for all biometric data captured by USCIS in furtherance of immigration benefit requests. BSS will facilitate the biometric-based background checks by utilizing direct links to the FBI's IAFIS network and US-VISIT/IDENT database. An encrypted web-based user interface will allow USCIS adjudicators to electronically submit and/or resubmit fingerprints to the FBI. This will allow improvements in case adjudication and decrease the burden on immigration applicants/petitioners/beneficiaries (further referred to as applicants) by decreasing return visits to USCIS Application Support Centers (ASC) for additional biometric capture. In future releases, BSS

[1] 10-Prints consist of the following: rolled impression of each individual finger, flat impression of each individual thumb, flat impression of the four fingers (index, middle, ring, and little finger) for the right hand and left hand, separately, at a 45 degree angle.

will take advantage of features offered by the FBI and US-VISIT known as "wrap-back." Wrap-back will allow USCIS to submit only one set of fingerprints to both the FBI and US-VISIT/IDENT. The FBI and/or US-VISIT/IDENT will then notify USCIS should those fingerprints appear in subsequent encounters. An amendment to this PIA will be published prior to the implementation of this new functionality.

In its third role, BSS will become the centralized source of images used for USCIS benefit card and document production. BSS will interface with USCIS' National Production System II / Integrated Card Production System (NPS II/ICPS) and the Computer-Linked Application Information Management System (CLAIMS) 3 to transmit appropriate data for card production and receive card issuance status.

In its fourth role, BSS will facilitate biometrics based identity verification. Once an applicant's biometric data is stored in BSS, the identity can be verified through the US-VISIT/IDENT interface by comparing their fingerprint with the biometrics (fingerprint) originally submitted to BSS. This will eliminate the possibility of identity theft and significantly reduce the risk of fraud by allowing USCIS adjudicators to verify visually the applicant presenting the biometrics with the identity already on file.

BSS will help transition the agency's data management practices to a paperless, more centralized, and person-centric approach as part of a USCIS enterprise-wide "Transformation Program." The Transformation Program will be utilizing the Unique Enumeration program as a keystone for all future Transformation Program systems. The Unique Enumeration program assigns a unique enumerator to an individual's biometric and related biographic data. The unique enumerator will facilitate interaction between the individual and USCIS, simplify the processing of updating an individual's file, and improve data quality. This will also eliminate the possibility of identity theft and significantly reduce the risk of identity fraud. BSS is a key building block of the USCIS Transformation Program. The US-VISIT/IDENT Unique Enumeration program is a new program currently under development; however, BSS will utilize the unique enumerator once the program becomes operational. US-Visit will publish a separate Privacy Impact Assessment (PIA) for the US-VISIT/IDENT Unique Enumeration Program.

Information collected directly from the applicant at the Application Support Centers (ASC) includes fingerprint-based biometrics as well as photographs, signatures, and associated biographic information. The data will transmit from the ASC to BSS.

Card production status from CLAIMS-3 and NPS II/ICPS, fingerprint based background check results from the FBI and US-VISIT/IDENT, and the US-VISIT unique enumerator will be handled electronically through direct system-to-system interactions. End users will have access via the encrypted web-based user interface. The user interface will allow authorized USCIS, Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Department of State (DoS) personnel to access the information residing in BSS. ICE, CBP, and DoS users will have read only access.

In addition to storing the biometric data of applicants, BSS will store all related activity including:

- The date fingerprint checks were conducted
- The classification[2] of the fingerprint
- The date the image set was sent to card production (NPS II/ICPS)
- The date a benefit was denied
- The date the card was produced

[2] A classifiable 10-print means the FBI can use the 10-print image to conduct a fingerprint check. An unclassifiable 10-print means the FBI cannot use the 10-print image to conduct a fingerprint check.

BSS will support the modification of established USCIS processes and allow for marked improvement in those processes by creating a single repository for all USCIS biometric and card production information. In addition, BSS' incorporation into USCIS' Transformation Program initiative will help transition the agency's data management practices to a paperless, more centralized, and person-centric approach.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The information collected in BSS includes biometric and associated biographic data provided at the time of biometric capture at an ASC. The biometric data includes 10-print fingerprints captured by the electronic live scan device,[3] manually inked and scanned (digitized) FD-258 cards, photographs, and signatures. The biographic data includes: Alien Registration Number (A-Number); First and Last Name; Date of Birth; Country of Birth; Gender; Aliases; Height; Weight; Race; Class of Admission; Address; and other biographic data associated with applicants. The above data elements will assemble into the National Institute of Standard and Technology (NIS) approved Electronic Fingerprint Transmission Specification (EFTS) file for transmission from the ASC to BSS.

BSS will use the EFTS to submit a Fingerprint Check to the FBI. The results of the Fingerprint Check are returned to BSS, which are then interpreted as classifiable (usable) or unclassifiable (unusable). A classifiable fingerprint set denotes that the FBI was able to utilize the fingerprints in the course of their matching processes. An unclassifiable fingerprint set denotes that the FBI was unable to utilize the fingerprints in the course of their matching processes. The system will not store the FBI Identification Record (commonly referred to as a RAP Sheet) portion of the FBI Fingerprint Check Result file. BSS will route the RAP Sheet to the Background Check System (BCS) where it will be stored.

When the US-VISIT Unique Enumeration program becomes operational, BSS will be able to receive a unique enumerator for enrolled identities. BSS will submit 10-print fingerprints to US-VISIT using EFTS, which will then attempt to match the fingerprints with existing records. US-VISIT will return a unique enumerator to BSS if it finds a match.. US-VISIT will enroll the set of prints, generate a unique enumerator, and send it back to BSS if a match is not found.

Additionally, US-VISIT will search its IDENT database. US-VISIT/IDENT will return an information file if applicable. This file will route through BSS to BCS for storage.

BSS will also receive benefit card and document issuance data from NPS II/ICPS including but not limited to card serial number, receipt number, production site, production date, class of admission, type of benefit card or document, and expiration date.

[3] This is a generic term for electronic fingerprint machines.

1.2 From whom is information collected?

BSS has no direct interaction with the benefit applicant.

The information in BSS relating to the fingerprint biometrics is collected from the applicants of UCSIS benefits at the time of biometric capture. Fingerprints are obtained electronically at one of USCIS' Application Support Centers (ASC). Fingerprints may also be obtained from hard copy fingerprint cards (FD-258) for those applicants who are unable to submit 10-prints fingerprints electronically. Fingerprints are transmitted to BSS directly from the ASCs in an EFTS format, which are then submitted to the FBI.

BSS will receive the FBI Fingerprint Check Result file as a result of submitting 10-print fingerprint images. BSS will route this file, which includes the FBI RAP Sheet, to BCS. BSS will also use the file to interpret and store the FBI Fingerprint classification in BSS.

BSS will receive and store a unique enumerator from US-VISIT/IDENT as a result of submitting 10-print fingerprint images and associated biographic information. BSS will also receive the US-VISIT/IDENT information relating to a set of submitted 10-prints that yield a match in a law enforcement database. However, BSS will not store this file. BCS will store the US-VISIT/IDENT information. BSS may request updated US-VISIT/IDENT information by utilizing the unique enumerator as a search string, which would be routed to BCS for storage.

The information relating to benefit card and document production received from NPS II/ICPS will be stored in BSS and updated when applicable, for example, when new card production activity occurs.

Information will also be included from USCIS case management systems such as CLAIMS 3, which is used to process applications including, but not limited to, an Adjustment of Status (Green Card) and Employment Authorization Document (EAD).

As the USCIS Transformation Program progresses, new systems will interface with BSS. This PIA will be updated to reflect those new interfaces.

1.3 Why is the information being collected?

USCIS captures biometric data from applicants to facilitate three key operational functions: (1) conducting fingerprint-based background checks; (2) verifying an applicant's identity; and (3) producing benefit cards/documents. Currently, USCIS does not have a centralized, long-term storage program for fingerprint biometrics. Accordingly, applicants are sometimes required to return to an USCIS Application Support Center (ASC) to provide fingerprints again during the case adjudication process. BSS will store the biometric information, thereby decreasing the burden on applicants by negating the need to provide multiple sets of biometric data.

Further, BSS will consolidate storage of information from multiple, separate systems into a centralized database, allowing for greater control, security, and management of the data. BSS also will provide increased functionality over current systems, and improved communication between government databases and personnel, facilitating more efficient processing of applications. This furthers USCIS's goals of reducing immigration benefit and petition case backlog, and improving the process for vetting and resolving applications for immigration benefits.

1.4 How is the information collected?

Information is collected directly from applicants at the time of biometric capture at an ASC. This information includes fingerprint biometric data, photograph, signature, and associated biographic information. All information is transmitted from the electronic live scan devices to BSS.

USCIS employees/contractors may obtain information by providing remote fingerprint and data collection services worldwide. USCIS personnel travel to refugee camps to capture applicant biometrics. Due to the remote locations, infrequent, and/or unstable conditions, this data is sometimes transferred to Compact Disk (CD) and mailed (e.g., certified carrier, diplomatic pouch) or carried back to USCIS Headquarters for processing. The data contained on CDs is encrypted with the National Institute of Standards and Technology (NIST) 256-bit Advanced Encryption Standard (AES) algorithm. The passwords to decrypt the transmitted CDs are sent via a separate communication channel. When the data arrives at USCIS Headquarters, the information is decrypted, loaded onto a DHS approved workstation and uploaded to BSS for processing.

Results from fingerprint based background checks, card production status, and the unique enumerator will be received from the FBI IAFIS, US-VISIT/IDENT, CLAIMS 3, NPS II/ICPS, and BCS utilizing transaction IDs to match data accurately.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The legal authority to collect this information comes from 8 U.S.C. § 1101 et seq.

In addition, the U.S. Office of Management and Budget (OMB) must approve the format of every public form available from USCIS and authorizes USCIS to collect the requested information on the forms. Lastly, USCIS has signed Memoranda of Understanding (MOUs) with the FBI and US-VISIT that set forth the terms and conditions for the transfer and use of information pertaining to background checks and associated with the interaction with the FBI and US-VISIT.

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

USCIS has created the system to improve the accuracy of biometric information received from applicants for verification purposes. The system will be used to consolidate information from multiple, disparate, systems into one centralized system. Data consolidation will allow for greater control over the security and management of data. The consolidation and centralization will allow for more accurate and efficient audit log monitoring to ensure that data is not misused or inappropriately disseminated.

The collection of information presents inherent privacy risks including the possible misuse and inappropriate dissemination of data. USCIS will develop and implement BSS in accordance with DHS approved security guidelines. Only users who need the information to effectively perform their job functions will gain access to BSS. All authorized users must go through an approval process and can only access BSS through DHS approved equipment. Lastly, all USCIS adjudicators who will be using BSS during the adjudication process have received the Federal Law Enforcement Training Center (FLETC) Freedom of Information Act/Privacy Act (FOIA/PA) training authored by the FLETC Legal Division.

Another risk source is assumed when USCIS personnel travel to worldwide refugee camps to capture applicant biometric and biographic data. The risk of remote data capture has been mitigated by deploying encryption at each point in the process. The entire laptop hard drive is encrypted and is useless without proper authentication credentials. When data is taken off of the laptop and placed onto a CD, the data is encrypted.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

USCIS will use the fingerprint biometric information to conduct background checks through the FBI IAFIS and US-VISIT/IDENT. Associated biographic information collected at the time of fingerprint biometric capture will be used to aid in positively identifying the correct individual's records. Fingerprint biometric information will be used to find the associated US-VISIT/IDENT unique enumerator if one previously exists. If the unique enumerator does not exist, US-VISIT will enroll the set of prints, generate a unique enumerator, and send it back to BSS.

USCIS will use the unique enumerator to track and reconcile all data pertaining to a specific applicant.

USCIS will send image sets (photograph, press prints, and signature) and biographic information to NPS II/ICPS for use in benefit card and document production.

USCIS management may use transactional data stored in BSS to create reports that provide an accurate profile of the fingerprint-based biometric background check and card production processes from several different perspectives. With this uniformly presented information, USCIS will be able to actively and effectively manage these processes, identify issues before they become problems, and strategically plan and implement new measures to support USCIS's broader mission.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. BSS will not be used for data mining.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

USCIS will enter the information from CLAIMS 3, NPS II/ICPS, US-VISIT/IDENT, FBI IAFIS, and biometric capture at the ASC directly into BSS via electronic interfaces. The data will be checked for accuracy and proper formatting during the electronic exchange. US-VISIT/IDENT will generate and/or return a unique enumerator for each identity enrolled in the system. Identity is established when the first set of applicant submitted 10-prints is enumerated, each subsequent encounter will be matched to the preexisting identity. This matching will ensure that the biometric and associated biographic information submitted only applies to one person. The unique enumerator will enable USCIS to identify an individual's record in BSS, US-VISIT/IDENT, and, in the future, other systems. Furthermore, US-VISIT and USCIS will conduct integrity checks to ensure that the system is matching the correct data.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

USCIS will attribute fingerprint biometric-based background check request and result records to the correct applicant file by matching the unique enumerator and other fields such as A-Number. USCIS will conduct integrity checks at all points of data transfer to ensure that USCIS has accurately matched the appropriate records and properly formatted the records before being stored. Further, all information will reside on secured networks and servers, with access limited to authorized personnel only. Lastly, USICS maintains audit logs in order to track and identify unauthorized use of system information. Information, including the user's name, date, and time of every transaction, will be stored in a log. If USCIS suspects misuse of data, these logs can be used to review and analyze all activity in BSS. Reporting from employee and/or system monitoring could identify the misuse of data. All BSS users will be notified that BSS stores these logs and USCIS management can use them to review all activity in BSS.

Section 3.0 Retention

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

BSS will store data for 75 years from the last recorded action. At some point during the 75 years, the records may be archived. BSS is replacing ISRS and will be using the approved retention period as a model for filing its retention request with NARA.

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

USCIS will submit the required "Request for Records Disposition Authority" (SF-115) form for approval by NARA. This form is the official request for approval of the proposed retention schedule. BSS will use ISRS's approved retention period as a model for filing its retention request.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

This information is needed for the indicated time because the relationship between an applicant and USCIS may span the 75 years that the data is retained. USCIS will use the historical data in BSS in the adjudication of applications/petitions in the future. BSS adopted the retention schedule of 75 years from the official disposition guidelines for a USCIS Alien File ("A-File"). The A-file is the physical paper file containing all correspondence and documentation, including all applications, petitions, reports, interview notes, and other written communications for every applicant.

The ability to forge identities is a growing concern and keeping this biometric and biographic data on record for lengthy periods can help protect against fraudulent benefit applications. USCIS has implemented several measures to combat identity fraud and facilitate the storage of all biometric and associated biographic data in BSS and US-VISIT/IDENT for future use supports this initiative.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

BSS shares information internally with US-VISIT/IDENT for Unique Enumeration, biometric-based background checks, and storage purposes. Authorized CBP and ICE personnel may receive information from BSS either directly from USCIS personnel based upon possible fraudulent activity through the encrypted web-based user interface.

Additionally, information collected through BSS and stored in US-VISIT/IDENT will be shared with any other component in DHS where DHS determines that the receiving component has a need to know the information to carry out national security, law enforcement, immigration, intelligence, and other DHS-mission-related functions.

4.2 For each organization, what information is shared and for what purpose?

After BSS captures 10-print fingerprints, they are transmitted to US-VISIT/IDENT with associated biographic information for matching. US-VISIT/IDENT will attempt to match the submitted fingerprint biometrics to those already on file. If a match is made, US-VISIT/IDENT will return the unique enumerator associated with the fingerprint biometrics, which will be subsequently stored in BSS. If a match is not made, US-VISIT/IDENT will enroll the fingerprint biometrics, assign a unique enumerator and return the data to BSS for storage. Further, US-VISIT/IDENT will return an information file, if applicable, to BCS, which will store the US-VISIT/IDENT information file.

US-VISIT/IDENT will store all biometric and biographic data transmitted from BSS. US-VISIT/IDENT will use the information to record the arrival and departure of aliens; conduct certain terrorist and criminal checks on aliens; and verify alien's identity by comparing of biometric identifiers. US-VISIT will share this information with CBP and other DHS components after US-VISIT determines that the receiving component has a need to know the information to carry out national security, law enforcement, immigration, intelligence, and other DHS mission-related functions that are consistent with the purposes of the collections as stated in the System of Records Notice for BSS.

CBP and ICE will be able to access the encrypted web-based user interface to view biometric and biographic data in order to verify the identity of a person and validity of a USCIS issued travel document being presented at a port of entry, for example.

4.3 How is the information transmitted or disclosed?

BSS and US-VISIT/IDENT will communicate over a secure and reliable electronic interface using US-VISIT's proprietary Extensible Markup Language (XML) standard. This interface will utilize secure network connections on the DHS core network. BSS will send 10-print fingerprint biometrics and biographic information to US-VISIT/IDENT via this interface. US-VISIT/IDENT will return a unique enumerator that will be stored in BSS to identify records via this interface.

When fingerprints submitted to US-VISIT/IDENT yield a match, US-VISIT/IDENT will send the information file to BSS via this interface. BSS will not store this file but will flow to BCS for storage.

CBP and ICE will be given read only access to BSS through the web-based interface. Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, "Safeguarding Personally Identifiable Information," dated May 22, 2006 and M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006 setting forth the standards for the handling and safeguarding of personally identifying information. Contractors must also sign non-disclosure agreements.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Internal sharing of data is conducted over secured networks controlled by DHS utilizing DHS approved computers, services, and software. The privacy risks associated with each step of internal sharing, including system and network security, data usage, data transmission, and disclosure have been identified and mitigated through adherence to DHS policies and procedures such as System Design Life Cycle documentation and Certification and Accreditation documentation. In addition, only authorized users who need the information contained in BSS have access to the system.

There will always be the possibility of misuse and inappropriate dissemination of information despite the above described technical security aspects. Security logs, audit logs of user activity, and strict access controls will be enforced to help mitigate these risks. Users will be given access to the system only after the user's supervisor and the Password Issuance Control System (PICS) officer have authorized an account request form. Further risk exists with US-VISIT allowing other agencies to search USCIS data; however, these risks are mitigated by US-VISIT's successful completion of all DHS system certification and privacy compliance processes.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

When operational, BSS shares information externally with the FBI for FBI Fingerprint Background Checks purposes. BSS also shares information externally with the Department of State (DoS).

In the future, US-VISIT may share USCIS's biometric and biographic data with the Central Intelligence Agency (CIA) and National Counter Terrorism Center (NCTC) for national security and counterterrorism purposes. US-VISIT may also share data with foreign immigration agencies to assist them in making immigration benefit determinations well as for foreign countries' national security purposes, but only to the extent permissible by law.

5.2 What information is shared and for what purpose?

BSS will receive the fingerprints from the ASCs in the EFTS format, consisting of fingerprints and associated biographic information, to submit to the FBI. BSS will electronically receive and store all FBI Fingerprint Check Requests.

BSS will interpret and store the FBI Fingerprint Check Result file for classification. If the FBI Fingerprint Check yielded a match, the FBI will return a copy of the RAP Sheet to BSS. The RAP Sheet information will be stored in BCS.

BSS will allow the DoS read-only access to view biometric and biographic information via the encrypted web-based user interface. DoS personnel will use the web-based interface to verify the identity of a person and validity of a USCIS travel document being presented at a U.S. consular office.

US-VISIT will share USCIS' biometric and biographic data to external agencies through the US-VISIT/IDENT interface. US-VISIT will allow the CIA, NCTC, and foreign immigration agencies access to the data. This data will be shared for immigration benefits and national security purposes, but only to the extent permissible by law. DHS/USVIST will only share the information after DHS determines that the receiving agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, and other DHS mission-related functions and consistent with the routine uses published in the System of Record Notice for BSS.

5.3 How is the information transmitted or disclosed?

FBI Fingerprint Check Requests and results are electronically transmitted through BSS to IAFIS over both DHS and FBI secure networks utilizing end-to-end encryption. The FBI will return results directly to BSS, which will interpret the classification based on the returned FBI Fingerprint Check Result file, then pass the RAP Sheet data on to BCS and encounter information on to US-VISIT/IDENT. All data will be encrypted and transmitted over DHS and DOJ secured networks. In the future, US-VISIT will share data with external intelligence agencies to conduct terrorism related activities. These agencies include the CIA and NCTC. US-

VISIT will also give access to foreign immigration agencies in Canada, the United Kingdom, and Australia. As additional data sharing requirements are implemented, amendments to the PIA will be published.

The DoS will access BSS via a secured web-interface. USCIS Biometric and Biographical information will be provided to the CIA, NCTC and to foreign immigration agencies through US-VISIT protocols.

5.4 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?

USCIS has existing MOUs with the FBI. The terms and conditions for the exchange of data used for Fingerprint Check purposes are defined in the MOUs between USCIS and the FBI. The MOUs also limit the use and re-dissemination of the information. MOUs will be in place reflecting USCIS' participation with US-VISIT's external data sharing practices before the sharing becomes active.

The FBI will store all 10-prints fingerprints submitted by USCIS pursuant to an agreement between the Executive Deputy Associate Commissioner, Immigration Services Division, U.S. Immigration and Naturalization Service (INS) and the Assistant Director, Criminal Justice Information Services Division (CJIS), FBI dated September 25, 2002. The FBI will keep these prints on file for the purpose of conducting fingerprint based background checks. The prints will be stored in the FBI's Civil Electronic File, which is covered in the FBI's Privacy Act Notice for the Fingerprint Identification Record System (FIRS) published on September 28, 1999.

An MOU is being drafted with the DoS to cover appropriate uses of USCIS systems and information.

Lastly, an MOU is being drafted with US-VISIT covering appropriate uses of USCIS systems and information when sharing with the CIA, NCTC, and foreign immigration agencies. This MOU will address specific confidentiality protections provided to certain classes of applicants for example, asylum seekers.

5.5 How is the shared information secured by the recipient?

The recipients of the shared information are the FBI, DoS, CIA, NCTC, and foreign immigration agencies. The information provided to the FBI, CIA, and NCTC by USCIS is restricted to employees with Top Secret clearances who work in secure buildings and on secure systems. The information provided to the DoS is restricted to authorized personnel who have gone through the account approval process and all applicable training. Information provided to foreign immigration agencies will be provided only to employees who have passed all required background checks as stipulated in the agreements signed between DHS and the foreign immigration agency.

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

Federal government employees and their agents must adhere to the OMB guidance provided in OMB Memoranda, M-06-15, "Safeguarding Personally Identifiable Information," dated May 22, 2006 and M-06-16 "Protection of Sensitive Agency Information," dated June 23, 2006 setting forth the standards for the handling and safeguarding of personally identifying information.

FBI employees who perform Fingerprint Checks have received the required training to perform the checks. DoS employees that need to access the system will be trained on how to use the system and how to handle USCIS data. CIA and NCTC employees will have proper training in handling sensitive information and pose valid Federal Government security clearances. Foreign immigration agency employees will be trained on how to handle sensitive data.

If deemed appropriate, proper data use training will be provided to CIA, NCTC, and foreign immigration agency users.

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

FBI Fingerprint Checks will be conducted over secured DHS and DOJ networks. Only authorized and trained FBI employees will handle biographic and biometric data. In addition, the FBI has policies and procedures in place to ensure that information is not inappropriately disseminated. Sharing data with DoS personnel will take place through the secured and encrypted web-based user interface. Data will only be provided to cleared personnel at US-VISIT, CIA, NCTC, and foreign immigration agencies. Appropriate policy checks have been put in place to ensure that the requesting agency has a need to know the information and that it is consistent with the routine uses laid out in the System of Records Notice.

There is a possibility of misuse and inappropriate dissemination despite the above technical security considerations. However, taking advantage of DHS Security specifications that require audit logs of user activity, security logs, and strict access controls mitigates these risks.

All user actions will be tracked via audit logs. However, privacy risks still exist, including misuse of data, theft of data, and/or compromise of data integrity. Designing the transmission system in accordance with DHS, OMB, and NIST guidelines for securing Sensitive but Unclassified (SBU) data have helped has mitigated these identified risks. These guidelines provide a baseline to data security and integrity that will be strictly followed in developing the system.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information? 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, why not?

A Systems of Records Notice (SORN) and PIA will be published for BSS. A Privacy Act Notice and a signature release authorization on the benefit application will notify applicants on the uses and sharing of the information collected by USCIS. One of the most widely used forms for capturing biometrics is the I-90 Application to Replace Permanent Resident Card. A copy of the form's Privacy Act Notice and signature release authorization has been attached as an appendix.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Applicants who apply for USCIS benefits are presented with a Privacy Act Notice and a signature release authorization on the benefit application/petition. The Privacy Act Notice details the authority and uses of information the applicant will provide on the USCIS benefit application/petition. The form also contains a signature certification and authorization to release any information from an applicant record that USCIS needs to determine eligibility. It is within the rights of the applicant to decline to provide the required information; however, it will result in the denial of the applicant's benefit request.

USCIS benefit applications/petitions require that certain biographic information be provided and may require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision to grant or deny a USCIS benefit. The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit. Therefore, through the application process, individuals have consented to the use of the information submitted for adjudication purposes including background investigations.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

A Privacy Act Notice detailing authority and uses of information is presented to the applicant. The form also contains a signature certification and authorization to release any information from an applicant record that USCIS needs to determine eligibility, which includes biometric and biographic information.

All USCIS application and petition forms include a Privacy Act Notice and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…"

The applicant provides consent when an application/petition is signed to release any information that will be used to determine eligibility.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The collection of personally identifiable information is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk associated with this particular collection of information involves the applicant not being fully aware that their information will be used to conduct a background investigation. USCIS has provided a Privacy Act Notice on benefit application/petition forms in order to mitigate this risk. The form also contains a signature certification and authorization to release any information provided by an applicant. USCIS is issuing this PIA and the associated SORN to mitigate this risk further.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The applicant can file a Freedom of Information Act (FOIA)/Privacy Act (PA) request to gain access to their USCIS record. USCIS has final discretion on withholding or releasing the requested information.

If an individual would like to file a FOIA/PA request to view their USCIS record, the request can be mailed to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

Further information for FOIA requests for USCIS records can also be found at http://www.uscis.gov.

7.2 What are the procedures for correcting erroneous information?

All data in BSS is obtained from previously entered data from the systems listed in Section 1.2. If an individual would like to correct known erroneous information in their USCIS record, the individual can file a USCIS form directed at changing the specific erroneous information. For example, an applicant can update their name by filing an Application to Replace Permanent Resident Card (I-90). After this form is processed, the changes will reach BSS through one of the systems listed in Section 1.2 and all relevant fields will be updated in BSS. If an applicant believes their file is incorrect but does not know which information is erroneous, the applicant may file a FOIA/PA request as detailed in Section 7.1.

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

Individuals are notified of the procedures for correcting their information on USCIS forms, the USCIS website and by USCIS personnel who interact with benefit applicants.

7.4 If no redress is provided, are alternatives are available?

Normal USCIS procedure for redress is provided to applicants as outlined in Sections 7.1 and 7.2.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The data contained within BSS is obtained from the systems listed in Section 1.2, and as such, individuals must address all information access rights to these systems. Previously established procedures for changing biographical information can be followed to correct known erroneous information, for example filing an I-90 form to change an applicant's/petitioner's address and have a new benefit card or document produced. If the applicant suspects erroneous information but does not know which part of the information is incorrect, the applicant can file a FOIA/PA request as detailed in section 7.1.

Section 8.0
Technical Access and Security

8.1 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.)

Access will be limited to authorized USCIS employees and contractors as well as authorized and cleared CBP, ICE, and DoS employees. BSS will offer the following four levels of access: Operational, General, Management and System Administration, which are all detailed in Section 8.3. System access will be commensurate with job function. BSS does not offer public access.

8.2 Will contractors to DHS have access to the system?.

Yes. Contractors are used to maintain systems and to provide technical support. All contractors are required to pass a background check before receiving access to a DHS building or system. All information technology (IT) based contracts must have Privacy Act compliance language present before being awarded according to DHS contracting guidelines based on the Federal Acquisition Regulation and other Executive Orders, public law and national policy. All access to the BSS system follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. There will be four user classes for BSS:

- Class 1 – Operational – Users requiring read only access to all data and images stored in the system;
- Class 2 – General – Users requiring access to view and resubmit biometric data;
- Class 3 – Management – Users requiring all standard functions and ability to run Reports; and
- Class 4 – System Administration – Users requiring system administrative privileges.

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

A standard request form (G-872B) must be completed by each user and authorized by a supervisor in that department and by the system owner's representative.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

BSS will maintain activity logs including transactions by users. Reports can be run to verify that a user's activity is consistent with their permissions.

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

BSS contains audit trail records to resubmit, review, and examine the originally submitted Fingerprint Check request, card production requests, and the results. Fingerprint Check request data may be resubmitted based on expired FBI Fingerprint Check results. Audit trails will ensure that the Fingerprint Check Request data is not duplicated. All BSS transactions are subject to monitoring and review to ensure that the original requests or results data are not lost, manipulated, or compromised in any manner. Audit trails will also be kept for BSS user activity. Lastly, secured DHS and FBI Networks will be used for data transmission between USCIS, the FBI, and US-VISIT to ensure that data has not been tampered with and to prevent unauthorized personnel from viewing the data.

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

Training on the BSS system will be provided to BSS users. This training will address appropriate privacy concerns. In addition, USCIS employees and contractors who have completed a G-872B form (see Section 8.4) and granted appropriate access levels (see Section 8.3) by a supervisor will be assigned a login and password from PICS to access the system. These users will have previously undergone federally approved clearance investigations and signed appropriate documentation in order to obtain the appropriate access levels. In addition, every Federal employee and contractor is required to complete computer security awareness training annually.

8.8 Is the data secured in accordance with Federal Information Security Management Act (FISMA) requirements? If yes, when was Certification & Accreditation last completed?

The BSS Team is currently engaged in the Certification and Accreditation process with the appropriate USCIS Office of Chief Information Officer security staff. The system will have an Authority to Operate (ATO) before it is made operational.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users will be broken into specific classes with specific access rights. Audit trails will be kept in order to track and identify any unauthorized use of system information. Data encryption will be employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, BSS complies with DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack, and unauthorized information dissemination.

Section 9.0
Technology

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

The system was designed with both commercial off-the-shelf products and custom designed software, databases, and user interfaces.

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

BSS developers followed the DHS System Development Life Cycle 6.0 security guidelines in the design and development of BCS. All documentation has been reviewed and approved by USCIS Information Technology (IT) Security. Fingerprint background check request and result records will be attributed to the correct applicant file by matching the unique enumerator and other data points including A-Number, Receipt Number, Last Name, and Date of Birth. BSS data integrity checks were designed based on a detailed analysis of data sources (see Section 1.2) and specific data elements coming into BSS. In addition to these integrity controls, the system was designed to acknowledge successful and failed data deliveries to ensure that data is never lost in transit. Further, for interaction with the systems listed in Section 1.2, all requests will contain a correlation identifier that will be used to match the results with the proper request.

9.3 What design choices were made to enhance privacy?

BSS will be available to cleared USCIS, ICE, CBP, DoS employees, and USCIS contractors with appropriate security and access controls. The general public will not have access to the system. Protection and integrity of data, security and privacy are of paramount concern. The system follows all DHS Security guidelines for enhanced security, including the Certification and Accreditation security documents, Federal Information Processing Standards (FIPS) 199, Federal Information Security Management Act (FISMA), Trusted Agent-Federal Information Security Management Act (TA-FISMA), Office of Management and Budget (OMB) memoranda, and the National Institute of Standards and Technology (NIST) security guidelines.

The system will provide for more efficient management of USCIS fingerprint-based background check and card production processes by creating a centralized system to hold all biometric data and associated biographic data. The ability to track data and user activities though audit logs on a consolidated system is far easier and provides better accountability than tracking information across multiple systems.

Conclusion

BSS facilitates the USCIS fingerprint background check and card production processes. USCIS conducts fingerprint background checks on applicants during benefit adjudication. BSS provides centralized electronic routing, storage and processing of Fingerprint Check Requests and Results and card production image sets and data. The applicant data used in creating Fingerprint Check Requests is transmitted directly from image capture at an ASC to BSS in the EFTS format. BSS will submit the EFTS file to the FBI for a Fingerprint Check. Results from the FBI Fingerprint Check will be returned to BSS where the classification interpretation will be stored in BSS and RAP Sheet data will be routed to BCS. BSS will store the basic biographic information needed to identify an applicant and all transactional FBI Fingerprint Check Request and Result data associated with that applicant.

Additionally, BSS will submit 10-print fingerprint images to US-VISIT/IDENT along with associated biographic information. BSS will receive a unique enumerator from US-VISIT/IDENT along with a corresponding information file. BSS will store the unique enumerator and route the information file to BCS for storage.

BSS addresses privacy concerns in many ways, including the following:

- Consolidating multiple data storage locations to one centralized repository that will be easier to secure, manage, and monitor;
- Granting access to pre-approved USCIS employees and contractors as well as cleared CBP, ICE, and DoS employees;
- Auditing transaction records to ensure that requested information and result data are not manipulated or compromised;
- Providing BSS users with training that addresses privacy concerns; and
- Drafting a PIA and SORN that states USCIS' intentions for the use of the private information data collected from USCIS applicants. This will be shared with the public upon publication in the *Federal Register*.

BSS is a multi-phased project that is currently in its first phase. As future phases are developed, this PIA and associated SORN will be revised to address those updates as necessary.

Responsible Officials

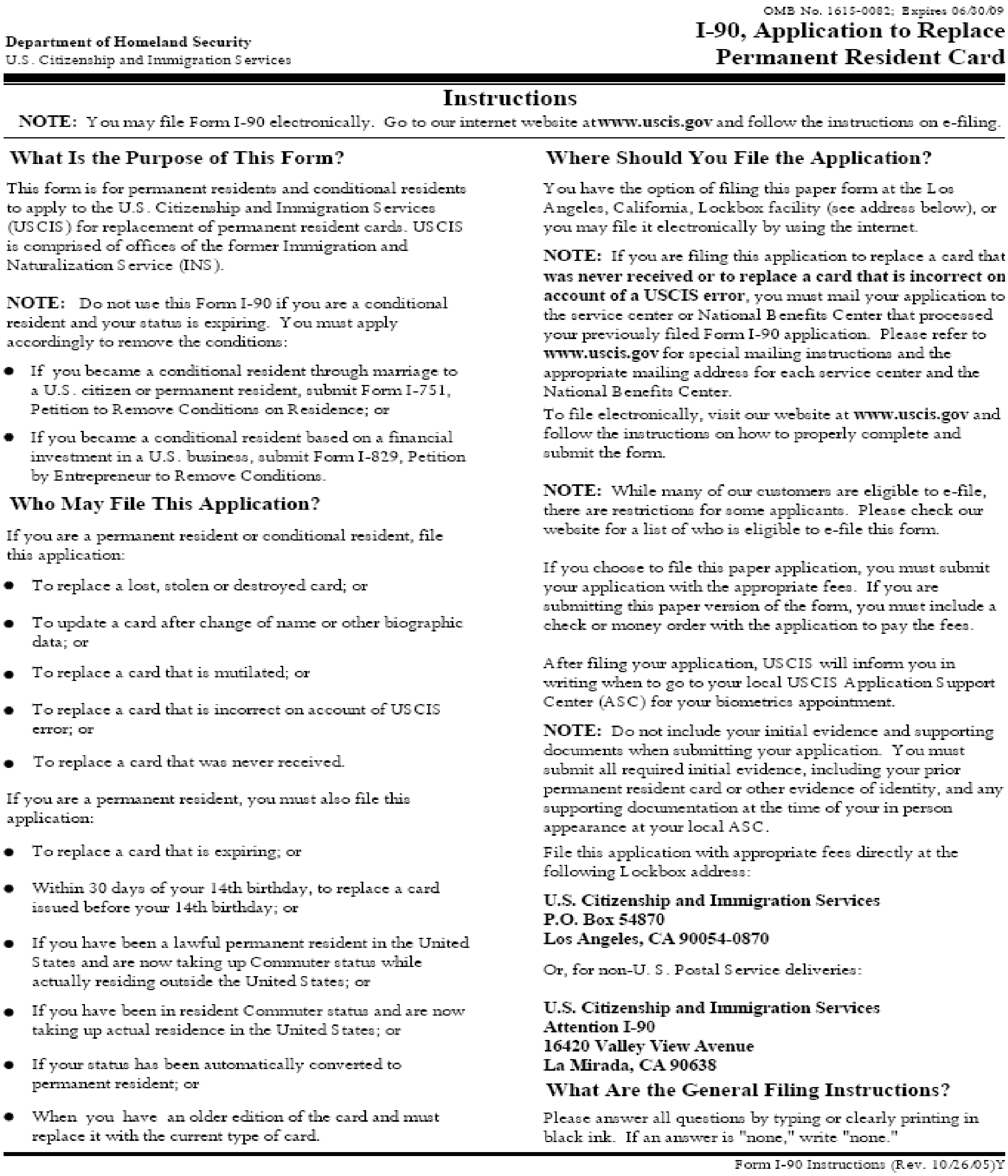
Elizabeth Gaffin, USCIS, Privacy Officer

Department of Homeland Security

Approval Signature Page

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A
I-90, Application to Replace Permanent Resident Card



OMB No. 1615-0082; Expires 06/30/09

Department of Homeland Security
U.S. Citizenship and Immigration Services

I-90, Application to Replace Permanent Resident Card

Instructions

NOTE: You may file Form I-90 electronically. Go to our internet website at **www.uscis.gov** and follow the instructions on e-filing.

What Is the Purpose of This Form?

This form is for permanent residents and conditional residents to apply to the U.S. Citizenship and Immigration Services (USCIS) for replacement of permanent resident cards. USCIS is comprised of offices of the former Immigration and Naturalization Service (INS).

NOTE: Do not use this Form I-90 if you are a conditional resident and your status is expiring. You must apply accordingly to remove the conditions:

- If you became a conditional resident through marriage to a U.S. citizen or permanent resident, submit Form I-751, Petition to Remove Conditions on Residence; or
- If you became a conditional resident based on a financial investment in a U.S. business, submit Form I-829, Petition by Entrepreneur to Remove Conditions.

Who May File This Application?

If you are a permanent resident or conditional resident, file this application:

- To replace a lost, stolen or destroyed card; or
- To update a card after change of name or other biographic data; or
- To replace a card that is mutilated; or
- To replace a card that is incorrect on account of USCIS error; or
- To replace a card that was never received.

If you are a permanent resident, you must also file this application:

- To replace a card that is expiring; or
- Within 30 days of your 14th birthday, to replace a card issued before your 14th birthday; or
- If you have been a lawful permanent resident in the United States and are now taking up Commuter status while actually residing outside the United States; or
- If you have been in resident Commuter status and are now taking up actual residence in the United States; or
- If your status has been automatically converted to permanent resident; or
- When you have an older edition of the card and must replace it with the current type of card.

Where Should You File the Application?

You have the option of filing this paper form at the Los Angeles, California, Lockbox facility (see address below), or you may file it electronically by using the internet.

NOTE: If you are filing this application to replace a card that **was never received or to replace a card that is incorrect on account of a USCIS error,** you must mail your application to the service center or National Benefits Center that processed your previously filed Form I-90 application. Please refer to **www.uscis.gov** for special mailing instructions and the appropriate mailing address for each service center and the National Benefits Center.

To file electronically, visit our website at **www.uscis.gov** and follow the instructions on how to properly complete and submit the form.

NOTE: While many of our customers are eligible to e-file, there are restrictions for some applicants. Please check our website for a list of who is eligible to e-file this form.

If you choose to file this paper application, you must submit your application with the appropriate fees. If you are submitting this paper version of the form, you must include a check or money order with the application to pay the fees.

After filing your application, USCIS will inform you in writing when to go to your local USCIS Application Support Center (ASC) for your biometrics appointment.

NOTE: Do not include your initial evidence and supporting documents when submitting your application. You must submit all required initial evidence, including your prior permanent resident card or other evidence of identity, and any supporting documentation at the time of your in person appearance at your local ASC.

File this application with appropriate fees directly at the following Lockbox address:

U.S. Citizenship and Immigration Services
P.O. Box 54870
Los Angeles, CA 90054-0870

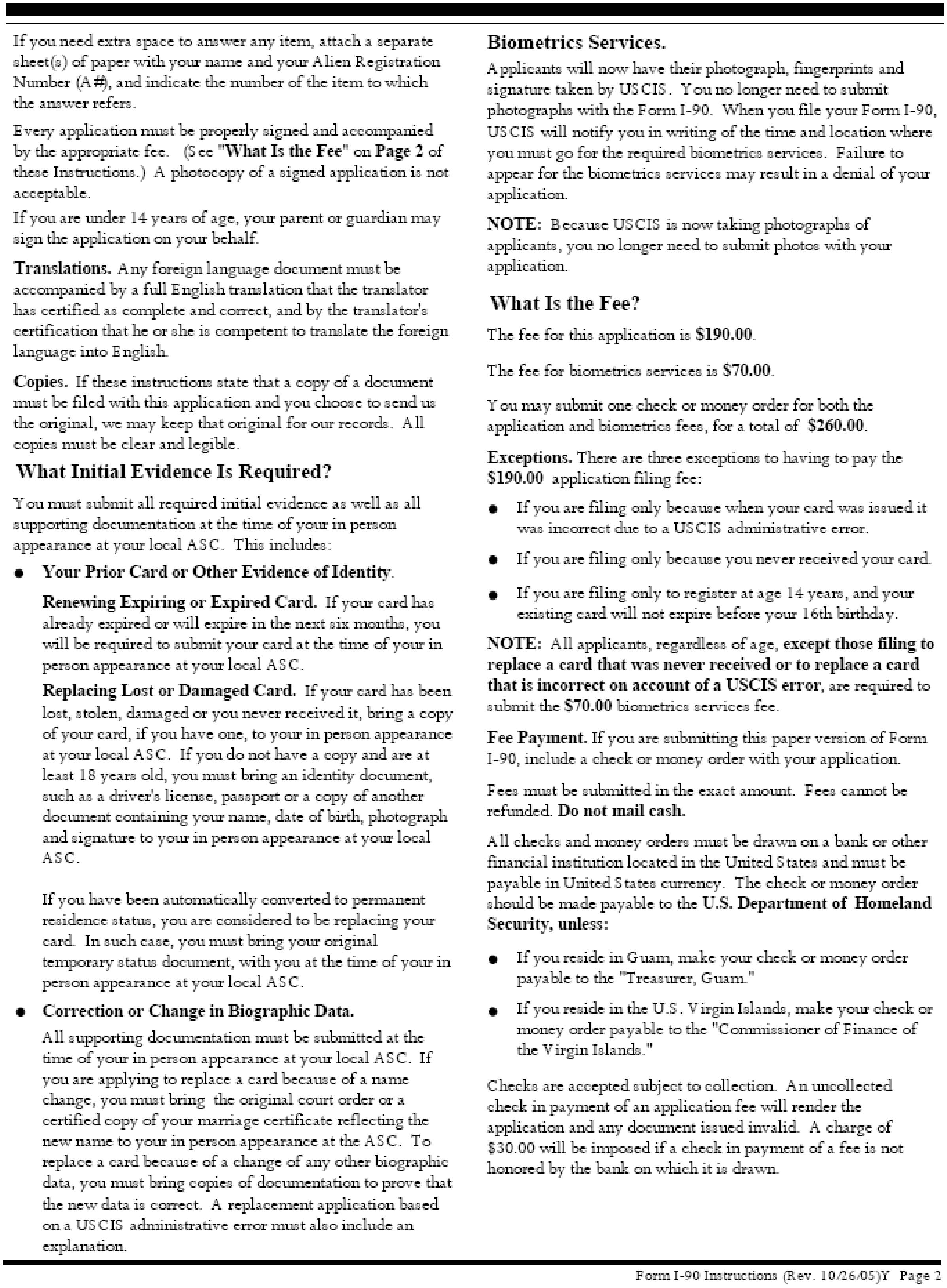
Or, for non-U. S. Postal Service deliveries:

U.S. Citizenship and Immigration Services
Attention I-90
16420 Valley View Avenue
La Mirada, CA 90638

What Are the General Filing Instructions?

Please answer all questions by typing or clearly printing in black ink. If an answer is "none," write "none."

Form I-90 Instructions (Rev. 10/26/05)Y



If you need extra space to answer any item, attach a separate sheet(s) of paper with your name and your Alien Registration Number (A#), and indicate the number of the item to which the answer refers.

Every application must be properly signed and accompanied by the appropriate fee. (See **"What Is the Fee"** on **Page 2** of these Instructions.) A photocopy of a signed application is not acceptable.

If you are under 14 years of age, your parent or guardian may sign the application on your behalf.

Translations. Any foreign language document must be accompanied by a full English translation that the translator has certified as complete and correct, and by the translator's certification that he or she is competent to translate the foreign language into English.

Copies. If these instructions state that a copy of a document must be filed with this application and you choose to send us the original, we may keep that original for our records. All copies must be clear and legible.

What Initial Evidence Is Required?

You must submit all required initial evidence as well as all supporting documentation at the time of your in person appearance at your local ASC. This includes:

- **Your Prior Card or Other Evidence of Identity**.

  Renewing Expiring or Expired Card. If your card has already expired or will expire in the next six months, you will be required to submit your card at the time of your in person appearance at your local ASC.

  Replacing Lost or Damaged Card. If your card has been lost, stolen, damaged or you never received it, bring a copy of your card, if you have one, to your in person appearance at your local ASC. If you do not have a copy and are at least 18 years old, you must bring an identity document, such as a driver's license, passport or a copy of another document containing your name, date of birth, photograph and signature to your in person appearance at your local ASC.

  If you have been automatically converted to permanent residence status, you are considered to be replacing your card. In such case, you must bring your original temporary status document, with you at the time of your in person appearance at your local ASC.

- **Correction or Change in Biographic Data.**

  All supporting documentation must be submitted at the time of your in person appearance at your local ASC. If you are applying to replace a card because of a name change, you must bring the original court order or a certified copy of your marriage certificate reflecting the new name to your in person appearance at the ASC. To replace a card because of a change of any other biographic data, you must bring copies of documentation to prove that the new data is correct. A replacement application based on a USCIS administrative error must also include an explanation.

Biometrics Services.

Applicants will now have their photograph, fingerprints and signature taken by USCIS. You no longer need to submit photographs with the Form I-90. When you file your Form I-90, USCIS will notify you in writing of the time and location where you must go for the required biometrics services. Failure to appear for the biometrics services may result in a denial of your application.

NOTE: Because USCIS is now taking photographs of applicants, you no longer need to submit photos with your application.

What Is the Fee?

The fee for this application is **$190.00**.

The fee for biometrics services is **$70.00**.

You may submit one check or money order for both the application and biometrics fees, for a total of **$260.00**.

Exceptions. There are three exceptions to having to pay the **$190.00** application filing fee:

- If you are filing only because when your card was issued it was incorrect due to a USCIS administrative error.
- If you are filing only because you never received your card.
- If you are filing only to register at age 14 years, and your existing card will not expire before your 16th birthday.

NOTE: All applicants, regardless of age, **except those filing to replace a card that was never received or to replace a card that is incorrect on account of a USCIS error**, are required to submit the **$70.00** biometrics services fee.

Fee Payment. If you are submitting this paper version of Form I-90, include a check or money order with your application.

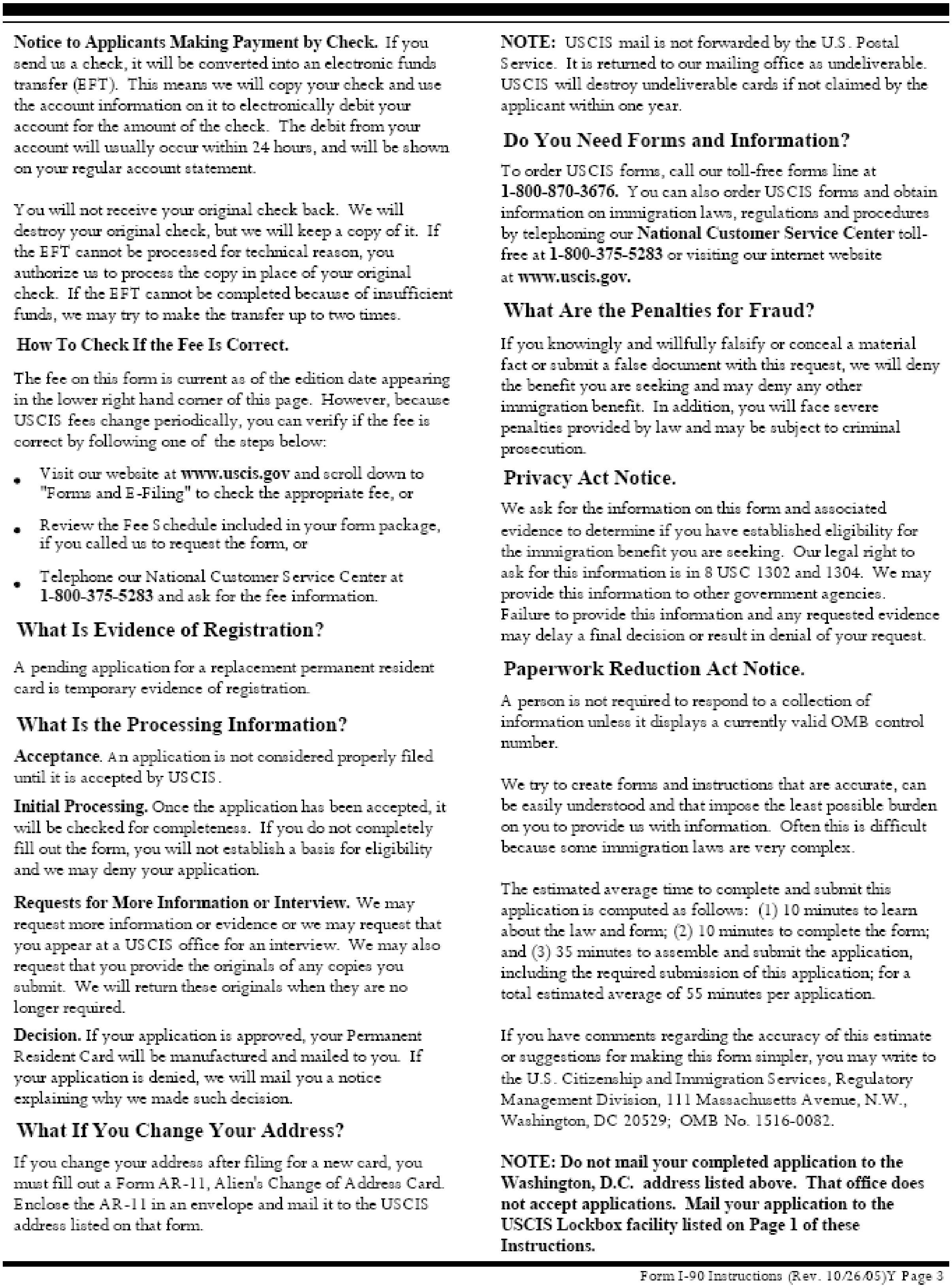
Fees must be submitted in the exact amount. Fees cannot be refunded. **Do not mail cash.**

All checks and money orders must be drawn on a bank or other financial institution located in the United States and must be payable in United States currency. The check or money order should be made payable to the **U.S. Department of Homeland Security, unless:**

- If you reside in Guam, make your check or money order payable to the "Treasurer, Guam."
- If you reside in the U.S. Virgin Islands, make your check or money order payable to the "Commissioner of Finance of the Virgin Islands."

Checks are accepted subject to collection. An uncollected check in payment of an application fee will render the application and any document issued invalid. A charge of $30.00 will be imposed if a check in payment of a fee is not honored by the bank on which it is drawn.

Form I-90 Instructions (Rev. 10/26/05)Y Page 2



Notice to Applicants Making Payment by Check. If you send us a check, it will be converted into an electronic funds transfer (EFT). This means we will copy your check and use the account information on it to electronically debit your account for the amount of the check. The debit from your account will usually occur within 24 hours, and will be shown on your regular account statement.

You will not receive your original check back. We will destroy your original check, but we will keep a copy of it. If the EFT cannot be processed for technical reason, you authorize us to process the copy in place of your original check. If the EFT cannot be completed because of insufficient funds, we may try to make the transfer up to two times.

How To Check If the Fee Is Correct.

The fee on this form is current as of the edition date appearing in the lower right hand corner of this page. However, because USCIS fees change periodically, you can verify if the fee is correct by following one of the steps below:

- Visit our website at **www.uscis.gov** and scroll down to "Forms and E-Filing" to check the appropriate fee, or
- Review the Fee Schedule included in your form package, if you called us to request the form, or
- Telephone our National Customer Service Center at **1-800-375-5283** and ask for the fee information.

What Is Evidence of Registration?

A pending application for a replacement permanent resident card is temporary evidence of registration.

What Is the Processing Information?

Acceptance. An application is not considered properly filed until it is accepted by USCIS.

Initial Processing. Once the application has been accepted, it will be checked for completeness. If you do not completely fill out the form, you will not establish a basis for eligibility and we may deny your application.

Requests for More Information or Interview. We may request more information or evidence or we may request that you appear at a USCIS office for an interview. We may also request that you provide the originals of any copies you submit. We will return these originals when they are no longer required.

Decision. If your application is approved, your Permanent Resident Card will be manufactured and mailed to you. If your application is denied, we will mail you a notice explaining why we made such decision.

What If You Change Your Address?

If you change your address after filing for a new card, you must fill out a Form AR-11, Alien's Change of Address Card. Enclose the AR-11 in an envelope and mail it to the USCIS address listed on that form.

NOTE: USCIS mail is not forwarded by the U.S. Postal Service. It is returned to our mailing office as undeliverable. USCIS will destroy undeliverable cards if not claimed by the applicant within one year.

Do You Need Forms and Information?

To order USCIS forms, call our toll-free forms line at **1-800-870-3676.** You can also order USCIS forms and obtain information on immigration laws, regulations and procedures by telephoning our **National Customer Service Center** toll-free at **1-800-375-5283** or visiting our internet website at **www.uscis.gov.**

What Are the Penalties for Fraud?

If you knowingly and willfully falsify or conceal a material fact or submit a false document with this request, we will deny the benefit you are seeking and may deny any other immigration benefit. In addition, you will face severe penalties provided by law and may be subject to criminal prosecution.

Privacy Act Notice.

We ask for the information on this form and associated evidence to determine if you have established eligibility for the immigration benefit you are seeking. Our legal right to ask for this information is in 8 USC 1302 and 1304. We may provide this information to other government agencies. Failure to provide this information and any requested evidence may delay a final decision or result in denial of your request.

Paperwork Reduction Act Notice.

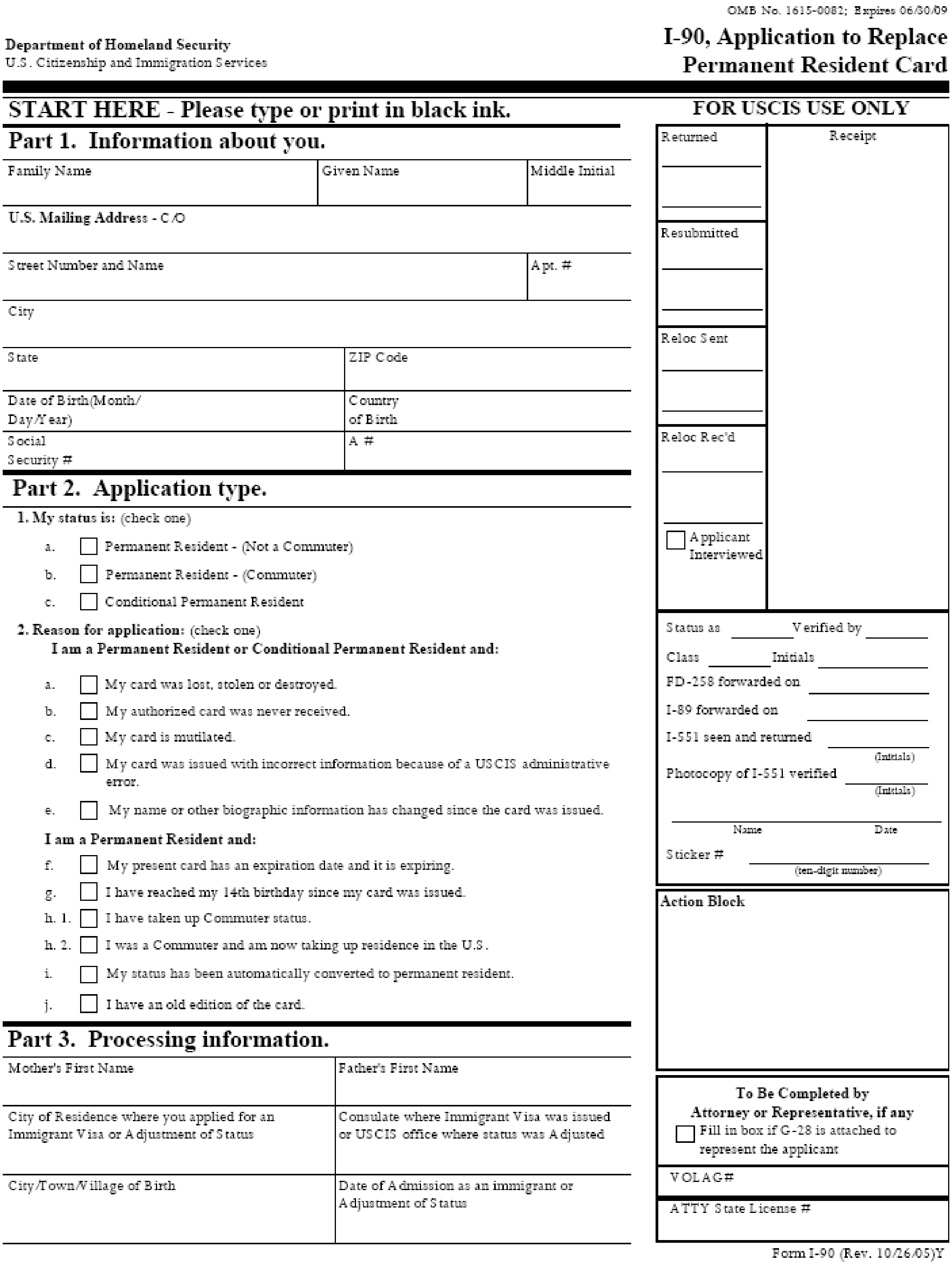
A person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

We try to create forms and instructions that are accurate, can be easily understood and that impose the least possible burden on you to provide us with information. Often this is difficult because some immigration laws are very complex.

The estimated average time to complete and submit this application is computed as follows: (1) 10 minutes to learn about the law and form; (2) 10 minutes to complete the form; and (3) 35 minutes to assemble and submit the application, including the required submission of this application; for a total estimated average of 55 minutes per application.

If you have comments regarding the accuracy of this estimate or suggestions for making this form simpler, you may write to the U.S. Citizenship and Immigration Services, Regulatory Management Division, 111 Massachusetts Avenue, N.W., Washington, DC 20529; OMB No. 1516-0082.

NOTE: Do not mail your completed application to the Washington, D.C. address listed above. That office does not accept applications. Mail your application to the USCIS Lockbox facility listed on Page 1 of these Instructions.



OMB No. 1615-0082; Expires 06/30/09

Department of Homeland Security
U.S. Citizenship and Immigration Services

I-90, Application to Replace Permanent Resident Card

START HERE - Please type or print in black ink.

FOR USCIS USE ONLY

Part 1. Information about you.

Family Name	Given Name	Middle Initial
U.S. Mailing Address - C/O		
Street Number and Name		Apt. #
City		
State	ZIP Code	
Date of Birth(Month/ Day/Year)	Country of Birth	
Social Security #	A #	

Part 2. Application type.

1. **My status is:** (check one)

a. □ Permanent Resident - (Not a Commuter)

b. □ Permanent Resident - (Commuter)

c. □ Conditional Permanent Resident

2. **Reason for application:** (check one)

I am a Permanent Resident or Conditional Permanent Resident and:

a. □ My card was lost, stolen or destroyed.

b. □ My authorized card was never received.

c. □ My card is mutilated.

d. □ My card was issued with incorrect information because of a USCIS administrative error.

e. □ My name or other biographic information has changed since the card was issued.

I am a Permanent Resident and:

f. □ My present card has an expiration date and it is expiring.

g. □ I have reached my 14th birthday since my card was issued.

h. 1. □ I have taken up Commuter status.

h. 2. □ I was a Commuter and am now taking up residence in the U.S.

i. □ My status has been automatically converted to permanent resident.

j. □ I have an old edition of the card.

Part 3. Processing information.

Mother's First Name	Father's First Name
City of Residence where you applied for an Immigrant Visa or Adjustment of Status	Consulate where Immigrant Visa was issued or USCIS office where status was Adjusted
City/Town/Village of Birth	Date of Admission as an immigrant or Adjustment of Status

Returned	Receipt
Resubmitted	
Reloc Sent	
Reloc Rec'd	
□ Applicant Interviewed	

Status as ________ Verified by ________

Class ________ Initials ________

FD-258 forwarded on ________

I-89 forwarded on ________

I-551 seen and returned ________
(Initials)

Photocopy of I-551 verified ________
(Initials)

____
Name Date

Sticker # ________
(ten-digit number)

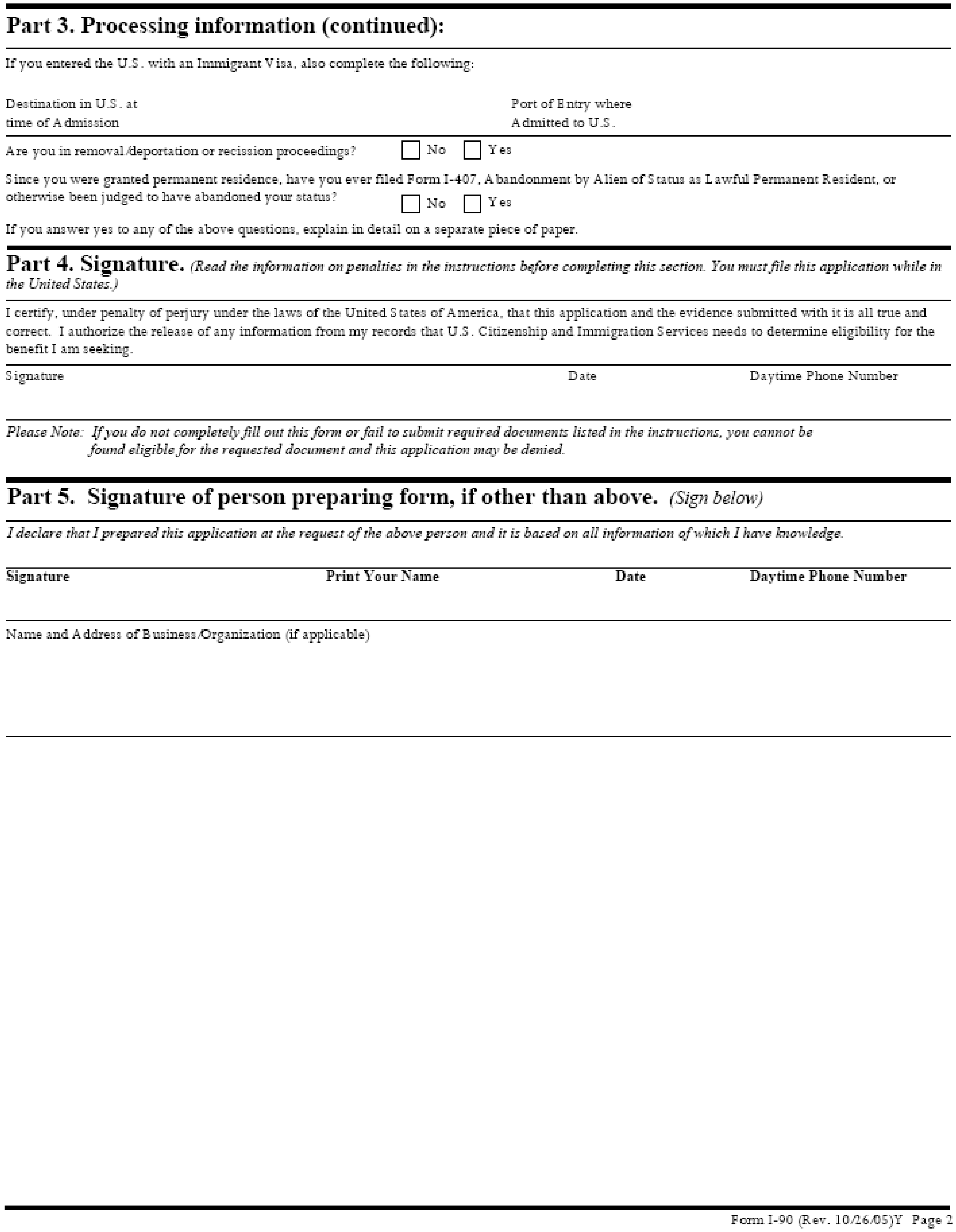
Action Block

To Be Completed by Attorney or Representative, if any
□ Fill in box if G-28 is attached to represent the applicant

VOLAG#

ATTY State License #

Form I-90 (Rev. 10/26/05)Y



Part 3. Processing information (continued):

If you entered the U.S. with an Immigrant Visa, also complete the following:

Destination in U.S. at time of Admission

Port of Entry where Admitted to U.S.

Are you in removal/deportation or recission proceedings? □ No □ Yes

Since you were granted permanent residence, have you ever filed Form I-407, Abandonment by Alien of Status as Lawful Permanent Resident, or otherwise been judged to have abandoned your status? □ No □ Yes

If you answer yes to any of the above questions, explain in detail on a separate piece of paper.

Part 4. Signature. *(Read the information on penalties in the instructions before completing this section. You must file this application while in the United States.)*

I certify, under penalty of perjury under the laws of the United States of America, that this application and the evidence submitted with it is all true and correct. I authorize the release of any information from my records that U.S. Citizenship and Immigration Services needs to determine eligibility for the benefit I am seeking.

Signature

Date

Daytime Phone Number

Please Note: If you do not completely fill out this form or fail to submit required documents listed in the instructions, you cannot be found eligible for the requested document and this application may be denied.

Part 5. Signature of person preparing form, if other than above. *(Sign below)*

I declare that I prepared this application at the request of the above person and it is based on all information of which I have knowledge.

Signature

Print Your Name

Date

Daytime Phone Number

Name and Address of Business/Organization (if applicable)

Form I-90 (Rev. 10/26/05)Y Page 2