Privacy Impact Assessment Update
for the

Alien Change of Address Card

(AR-11)

DHS/USCIS/PIA-018(b)

August 8, 2018

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Jonathan R. Cantor
Deputy Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Citizenship and Immigration Services (USCIS) is required to track address changes of individuals who have a pending or recently approved application, petition, or request form. USCIS is updating this Privacy Impact Assessment (PIA) for the Alien Change of Address Card (AR-11) to account for the modernization of the data systems that track change of address information.[1] USCIS is in the process of modernizing several systems, including AR-11, by retiring their mainframe applications and transitioning their operations and functions to a cloud environment. USCIS uses three independent systems to collect change of address information from individuals. The purpose of this PIA update to assess the privacy risks associated with migrating personally identifiable information (PII) from legacy AR-11 Mainframe to the cloud environment.

Overview

As set forth in Section 265 of the Immigration and Nationality Act (INA),[2] applicants, petitioners, and requestors who have a pending or recently approved application, petition, or request form are required to keep USCIS informed of their current mailing address. Change of address reporting is compulsory to allow USCIS to deliver notifications and otherwise communicate with individuals who have filed an application, petition, or request under the INA. In addition, USCIS may need to contact applicants, petitioners, and requestors to provide other documents, return original copies of evidence submitted to USCIS, or to request that additional documentation and evidence be provided pursuant to a request for evidence or notice of intent to deny.

USCIS offers the following methods for applicants, petitioners, and requestors to report a change of address:

1. **Mail**: Individuals may complete Form AR-11, *Alien's Change of Address Card,* by paper and mail it to USCIS.[3]
2. **Online:** Individuals may electronically complete and submit Form AR-11 through the online Customer Relationship Interface System (CRIS) Change of Address (CoA) module[4] or individuals may update their address through their secured online myUSCIS account.[5]

---

[1] *See* DHS/USCIS/PIA-018 Alien Change of Address Card (AR-11) and the associated update DHS/USCIS/PIA-018(a), *available at* https://www.dhs.gov/publication/alien-change-address-card-ar-11.
[2] 8 U.S.C. § 1305.
[3] Form *available at* https://www.uscis.gov/ar-11.
[4] *See* DHS/USCIS/PIA-019 Customer Relationship Interface System (CRIS), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cis_cris.pdf.
[5] *See* DHS/USCIS/PIA-071 myUSCIS Account Experience, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-myuscisaccountexperience-

3. **Telephone**: Individuals may call the National Customer Service Center and report a change of address.[6]

Change of Address IT Systems

USCIS uses three independent systems to collect change of address information from individuals, each of which corresponds to one of the three methods applicants, petitioners, and requestors can use to report the change. These systems are: (1) AR-11 Data Input System (AR-11/DIS), which is a temporary repository for paper submissions; (2) CRIS CoA, which facilitates telephone or electronic submissions; and (3) myUSCIS Account Experience for applicants, petitioners, and requestors with online accounts. The AR-11 Mainframe is primarily used in support of the AR-11/DIS and CRIS CoA systems to maintain and track address changes submitted to USCIS by non-U.S. citizens who are currently in the United States and who have submitted an electronic or paper Form AR-11. The AR-11 Mainframe maintains a one-way interface with both AR-11/DIS and CRIS CoA. Address changes made in the individual's secure myUSCIS online account only impact the filing submissions processed through USCIS ELIS,[7] and do not satisfy the INA requirement to keep addresses up to date.[8]

Reason for the PIA Update

USCIS primarily relied on the legacy AR-11 Mainframe to track change of address records received through paper submissions via AR-11/DIS and telephone or electronic submissions via CRIS CoA. The AR-11 Mainframe operating system has become outdated since it was originally built and has been replaced by modern technology. USCIS migrated the legacy AR-11 Mainframe operating system to a cloud-based platform. This technological advancement does not impact the collection and use of records in AR-11, but modifies the way USCIS stores and maintains change of address records. AR-11 Mainframe is now simply referred to as AR-11.

On December 9, 2010, the Office for Management and Budget (OMB) released a "25 Point Implementation Plan to Reform Federal Information Technology Management," which required the Federal Government to immediately shift to a "Cloud First" policy.[9] The three-part OMB

december2017.pdf.
[6] *See* DHS/USCIS/PIA-054 National Customer Service Center, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-ncsc-july2014.pdf.
[7] *See* DHS/USCIS/PIA-056 USCIS Electronic Immigration System (ELIS), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-elisappendixaupdate-may2018.pdf.
[8] USCIS will be implementing a pop-up banner to be displayed when a customer changes his or her address in the secure myUSCIS online account, notifying him or her that the official AR-11 form should also be filed along with the update in myUSCIS.
[9] 25 Point Implementation Plan to Reform Federal Information Technology Management (December 9, 2010), *available at* https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

strategy on cloud technology revolves around using commercial cloud technologies when feasible, launching private government clouds, and utilizing regional clouds with state and local governments when appropriate.

When evaluating options for new IT deployments, OMB requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment.

USCIS is undergoing a legacy system modernization effort to align with the "Cloud First" policy in order to improve business operations. AR-11 was originally built using a legacy Mainframe system, and USCIS has since migrated the AR-11 Mainframe to the Amazon Web Services (AWS) cloud platform. AWS is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) used by USCIS to protect data in accordance with federal security guidelines.[10] AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[11] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. This migration does not impact the collection and use of PII in AR-11 from the previous legacy system. USCIS requires AWS to segregate AR-11 data from all other third-party data. The cloud-hosted AR-11 system absorbed legacy AR-11 Mainframe functionality and system interconnections. All existing change of address records from the legacy AR-11 Mainframe were transferred to the new cloud environment.

Privacy Impact Analysis

Authorities and Other Requirements

All non-U.S. citizens who are required to be registered with USCIS are also required to keep USCIS informed of their current address. Pursuant to Section 265 of the INA, USCIS applicants, petitioners, and requestors are required to report a change of address within 10 days of moving by submitting an electronic or paper Form AR-11 to USCIS.[12]

[10] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[11] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[12] 8 U.S.C. 1305.

The change of address process is covered under the DHS/USCIS-007 Benefits Information System (BIS) Systems of Records Notice.[13]

The AR-11 is covered as a minor system under the Central Index System (CIS 2)[14] accreditation boundary. CIS 2 is a major application that is currently undergoing the Authority to Operate (ATO) process. Upon completion, CIS 2 will be accepted into the Ongoing Authorization program. Ongoing Authorization requires CIS 2 to be reviewed on a monthly basis and maintain its security and privacy posture to maintain its ATO.

NARA approved the retention schedule N1-566-10-3 for the Form AR-11, AR-11 Mainframe, and AR-11/DIS.

USCIS collects the change of address information directly from the applicant through a completed Form AR-11, which is subject to the requirements of the Paperwork Reduction Act (PRA). DHS obtained OMB approval and the Form AR-11 OMB Control Number is 1615-0007.

Characterization of the Information

There are no changes to the characterization of information outlined in DHS/USCIS/PIA-018 AR-11.

Uses of the Information

This update does not impact the use of information in AR-11. USCIS continues to use AR-11 to track change of address records.

Notice

This PIA update provides general notice to the public that USCIS migrated change of address records to the cloud environment from a legacy operating system, thereby changing the information storage and maintenance practices by USCIS. USCIS continues to provide notice about the collection, use, and maintenance of information to individuals through the Privacy Notice and BIS SORN.[15]

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not have notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. USCIS provides notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice that the information may be stored in a cloud-based system at the time of collection. Regardless of

[13] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[14] *See* DHS/USCIS/PIA-009 Central Index System, and associated updates, *available at* https://www.dhs.gov/publication/dhsuscispia-009-central-index-system.
[15] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).

storage location of records, the change of address records in AR-11 are governed by USCIS controls over collection, use, and dissemination of their information.

Data Retention by the project

This update does not impact how long data is retained in AR-11. NARA approved the retention schedule N1-566-10-3 for the electronic and paper-based Form AR-11 and respective AR-11 systems on December 14, 2010. This retention schedule states that paper forms should be destroyed within 180 days of the information being manually entered into AR-11/DIS, which is a temporary repository. Records retained in AR-11/DIS are deleted after two years from the date of receipt. Change of address information is maintained and disposed of in accordance with the approved NARA Retention Schedule.

Information Sharing

This update does not impact information sharing practices with internal or external entities. USCIS continues to share information with internal and external entities as outlined in DHS/USCIS/PIA-018 AR-11.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. USCIS continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. U.S. citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, the request can be mailed to the following address:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Persons not covered by the Privacy Act or JRA are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence

Auditing and Accountability

USCIS ensures that practices stated in this PIA update comply with internal federal, DHS, and USCIS policies, including the USCIS privacy policies, standard operating procedures, orientation and training, rules of behavior, and auditing and accountability procedures. USCIS

employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. Users are required to complete an access request form that is approved by a supervisor before they are granted access. USCIS also implements Role Based Access Controls, which give each user a standard role and a standard set of permissions to prevent the user from accessing anything outside their assigned role. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users. The physical location of the servers in which AR-11 data is to be stored are specified in cloud services contracts that restrict storage locations for AR-11 data to the United States.

DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

Privacy Risk: There is a risk to security of the collected information because AR-11 data is stored on third-party servers and may not have been assessed by USCIS security compliance personnel to ensure compliance with federal IT security requirements.

Mitigation: Cloud Service providers are required to undergo the FedRAMP review process and cloud service providers must be FedRAMP-certified. Through this process, cloud service providers may be provisionally approved based on an approval process that sets overall government standards—not just DHS or USCIS policy. By using FedRAMP-certified providers, USCIS leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance.

In addition, all contracted cloud service providers must also follow DHS privacy and security policy requirements. Before using AWS, USCIS verifies through an independent risk assessment that AWS met all DHS and USCIS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the USCIS Federal Information Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance. As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

USCIS CIS 2, which includes AR-11, is part of the Ongoing Authorization Program. Previously, information system compliance reporting was based on "point in time" evaluations and systems with an authority to operate were re-evaluated on three-year cycles. Many USCIS systems are now participating in the Ongoing Authorization Program, which is a risk-based security authorization process that provides authorizing officials with near real-time insight into

the security posture of an information system. USCIS is continuously reviewing security and privacy risks.

Privacy Risk: There is a risk that AR-11 records can be accessed by unauthorized personnel since AR-11 now resides in AWS, a public cloud.

Mitigation: This risk is mitigated. Although AR-11 operates in a public cloud, it is separated from other public cloud customers. AR-11 operates in a Virtual Private Cloud, which is a private component to the public cloud. USCIS controls access to the systems within the cloud, not AWS.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Deputy Chief Privacy Officer
Department of Homeland Security