Privacy Impact Assessment Update
for the

Citizenship & Immigration Data Repository (CIDR)

DHS/USCIS/PIA-031(b)

October 30, 2019

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

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

Abstract

U.S. Citizenship and Immigration Services (USCIS) developed the Citizenship and Immigration Data Repository (CIDR) to enable authorized USCIS users to efficiently query multiple USCIS benefits administration systems from a single entry point. CIDR allows for the vetting of USCIS immigration request information for indications of possible immigration fraud and national security concerns, detecting possible fraud and misuse of immigration information or position by USCIS employees for personal gain or by coercion, and responding to requests for information (RFI) from the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) or the federal intelligence community (IC) and law enforcement community (LE) members that are based on classified criteria. USCIS is updating this Privacy Impact Assessment (PIA) to (1) document a change in CIDR's data sources and (2) redefine the Office of Security and Integrity's (OSI) use of CIDR.

Overview

U.S. Citizenship and Immigration Services (USCIS) collects, tracks, and stores large amounts of information related to administering and processing benefit requests for all immigrant and nonimmigrant benefits (hereafter referred to as "immigration requests"). USCIS maintains a number of electronic systems to facilitate these purposes. The Citizenship and Immigration Data Repository (CIDR) consists of replicated data from the USCIS IT source systems used to process immigrant and nonimmigrant applications and petitions, or other immigration requests. USCIS developed CIDR, hosted on Department of Homeland Security (DHS) classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel to perform federated searches of the data, as well as comprehensive analysis of large data sets, for the purposes of: (1) vetting USCIS immigration request information for indications of possible immigration fraud, public safety, and national security concerns; (2) detecting possible fraud and misuse of immigration information or position by USCIS employees; and (3) responding to requests for information (RFIs) from the DHS Office of Intelligence and Analysis (I&A) or law enforcement (LE) and the Intelligence Community (IC) that are based on classified criteria.

In its initial deployment, USCIS CIDR ingested data from Computer Linked Application Information Management System 3 (CLAIMS 3)[1] with the intent to add additional data sets incrementally, as described in the January 2017 PIA.[2] For efficiency purposes, USCIS relied on a

[1] CLAIMS 3 is an electronic case management application that tracks and manages the adjudication process for most immigration request filings with the exception of naturalization, intercountry adoption, and certain requests for asylum and refugee status. For more information, *see* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.
[2] *See* DHS/USCIS/PIA-031(a) CIDR, *available at* www.dhs.gov/privacy.

connection between CIDR and the Service Center Computer Linked Application Information Management System (SCCLAIMS) to receive the exact copy of the CLAIMS 3 data on a daily basis. USCIS also planned to rely on this connection to receive the future data sets beyond CLAIMS 3 (e.g., Central Index System). This connection enabled USCIS to use CIDR in support of the USCIS mission. For example, the USCIS Office of Security and Integrity (OSI) uses data from CIDR and its source system audit logs to conduct investigations of possible fraud and misuse of immigration information or position by USCIS personnel.

Reason for the PIA Update

USCIS is updating this Privacy Impact Assessment (PIA) to (1) document a change in CIDR's data sources and (2) redefine OSI's use of data from CIDR to identify indicators[3] of fraud or misrepresentation in the management or operations by USCIS personnel.

Updated CIDR Data Sources

USCIS previously relied on a connection between CIDR and SCCLAIMS to receive the CLAIMS 3 data set. With this update, CIDR now connects with the Enterprise Citizenship and Immigrations Services Centralized Operation Repository (eCISCOR), a collection of databases on the unclassified network that serves as both a data warehouse and data hub for systems requiring data from other systems for operations, as its primary data source to access CLAIMS 3 data and to access the planned future data sets.[4] eCISCOR stores incrementally updated copies of transactional source systems' data for use by DHS end-users for reporting, analytic, and data sharing purposes. USCIS relies on extracting data via eCISCOR, rather than directly from the source systems, to reduce disruptions to and strain on the source systems.

eCISCOR accesses source system data and translates it from the source system format to a readable format for consumption by CIDR using a cross-domain solution (CDS). The CDS facilitates the transfer of unclassified data from eCISCOR to CIDR on the classified network. USCIS configures an automated job that retrieves the unclassified data and facilitates its transfer to CDS. The CDS then extracts the data, validates, scans, and transfers it to the classified domain. The transferred data files are never copied by the CDS, and the CDS only logs "who, when, and what" was transferred.

USCIS is undergoing a legacy system modernization effort to achieve paperless processing of immigration requests, automation, and to improve business operations. As a result of this

[3] Indicators, sometimes referred to as triggers or policies, will be reviewed by internal USCIS oversight offices—or the DHS Insider Threat Oversight Group (ITOG)—to ensure adequate protection of employee privacy, civil rights, and civil liberties. *For more information see* DHS/ALL/PIA-052 DHS Insider Threat Program *and subsequent updates*, *available at* www.dhs.gov/privacy.
[4] *See* DHS/USCIS/PIA-023(b) eCISCOR, *available at* www.dhs.gov/privacy.

modernization, some of the systems originally identified as data sources for CIDR have been updated or replaced. For example, the previous DHS/USCIS/PIA-031(a) CIDR PIA discussed a future receipt of data from the Refugees, Asylum, and Parole System (RAPS) Asylum Pre-screening System (APSS). These systems have now been decommissioned and replaced by a modernized system known as Global.[5] Currently, CLAIMS 3 is the only data set ingested into CIDR. As the planned future data sets are ingested into CIDR, USCIS will update Appendix A of this PIA.

OSI's use of CIDR

DHS/USCIS/PIA-031(a) previously identified the OSI Protective Intelligence Branch (PIB) as a user of CIDR. Due to organizational changes within OSI, PIB is no longer being referenced as a sole user of CIDR. Instead, USCIS is updating this PIA to state that CIDR will be used by OSI in support of fulfilling the statutory requirements of Section 453 of the Homeland Security Act.[6]

In order to fulfill the requirements of Section 453(b)(2), USCIS is developing a means to detect instances of fraud or corruption in the management and operations of USCIS. For example, to proactively detect if/when USCIS Adjudications Officers and/or Supervisory Adjudications Officers are attempting to manipulate the immigration system, OSI seeks to use proactive analytical capabilities to identify anomalies across USCIS programs that might indicate corruption or fraud in the management or operations of USCIS.[7]

CIDR provides OSI with the ability to access information that in the past may have been extremely difficult or impossible to extract from legacy immigration benefit systems. Pursuant to its statutory obligation to identify insider fraud and corruption risk, OSI plans to use that information from CIDR as a faster and more efficient means of accessing and analyzing adjudications data. CIDR maintains limited information on the users of the underlying USCIS source systems through audit logs. Using the source system audit logs, OSI can use the data from CIDR to discover linkages in which an employee, either for personal gain or by coercion, may be attempting to manipulate the immigration system. USCIS has previously encountered employee and contractor manipulation that could have been identified earlier using data from CIDR. For example, a former USCIS contractor accepted bribes in exchange for replacing the names of legitimately-naturalized citizens in USCIS systems with the names of those who had offered him

---

[5] Global operates in a cloud-based environment, to serve as the primary IT case management system for the administration of affirmative asylum, Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203, withholding of removal under the terms of a settlement agreement reached in a class action, credible fear, and reasonable cases. *See* DHS/ALL/PIA-027 USCIS Asylum Division, *available at* www.dhs.gov/privacy.

[6] Pub. L. 107-296.

[7] OSI provides leadership in the management of security within USCIS to protect employees, facilities, assets, and information to advance the USCIS Mission by ensuring effective, efficient, and continual operations. OSI derives its authority from relevant sections of the Homeland Security Act of 2002 (Pub. L. 107-296 (a)(2) & (b)(2)).

bribes. The former contractor's activities were conducted after hours and on weekends in order to avoid detection. In another case, a former Supervisory Adjudicator accepted bribes in exchange for favorably adjudicating naturalization cases. It is unusual for a Supervisory Adjudicator to perform adjudications. The use of data from audit logs reveals patterns and trends that could reveal this type of employee misconduct.

OSI uses the data from CIDR to conduct its analytical process outside of CIDR, which will be documented in a forthcoming PIA. OSI is coordinating with related stakeholders to develop triggers[8] that, based on previous incidents, could indicate internal fraud or corruption. OSI's analysts will perform analytics on data from CIDR based on those patterns and refer anomalous incidents to the appropriate stakeholder (e.g., DHS Office of Inspector General, USCIS Office of Investigations,[9] USCIS Fraud Detection and National Security Directorate (FDNS)) for review and investigatory action, if necessary. Furthermore, upon identifying anomalies indicating a systemic risk to the immigration system, OSI will incorporate internal controls mechanisms designed to combat those risks into its annual self-inspection process.

Previously, the underlying systems audit logs were retrievable by the Performance Issuance and Control System (PICS) ID.[10] With this update, USCIS is expanding the source system user data fields that are searchable/retrievable in CIDR (e.g., Adjudicator/User ID, Last Name, First Name, Title, Location, First Line Supervisor, and Field Office Director). The expanded data elements are not new data elements. Rather, they are existing source system data elements that may now be used to retrieve information within the audit logs since the PICS ID is no longer used throughout the Department.

---

[8] Triggers will be created based off previous incidents. For example, USCIS can create triggers to identify any changes made to a closed case, changes to adjudicated fields during weekends, or unusual adjudication activity by supervisory employees, or any anomalous activity by users on USCIS systems when certain conditions are met. These triggers will allow for OSI to detect unusual activity and take action early on and automatically or manually review incidents to determine if the anomalous activity is indicative of an insider threat. USCIS will work with internal USCIS oversight offices—or the DHS Insider Threat Oversight Group (ITOG)—to ensure adequate protection of employee privacy, civil rights, and civil liberties when developing these triggers. For more information *see* DHS/ALL/PIA-052 DHS Insider Threat Program and *subsequent updates*, *available at* www.dhs.gov/privacy.

[9] In July 2018, USCIS announced the organizational realignment of the OSI Investigations Division (INV) to an independent office named the Office of Investigations (OI). OI protects and strengthens the integrity of USCIS programs and systems by thoroughly and objectively investigating allegations of employee misconduct and insider threats, including those with a counterintelligence connection.

[10] PICS, which issued the PICS ID, was fully decommissioned as of March 14, 2018. Therefore, all functions previously handled by PICS are now completed through the MyAccess.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authority to operate CIDR does not change with this update. The legal authorities supporting the collection of the information used by CIDR come from the Immigration and Nationality Act (INA) Immigration and Nationality Act, sections 101 and 103, as amended (8 U.S.C. § 1101 and 1103), and the regulations issued pursuant thereto; sec. 453 and 454 of the Homeland Security Act of 2002 (Pub. L. 107-296); Executive Order (E.O.) 12958, and as amended; E.O. 13388; and E.O. 12333, as amended.

The Citizenship and Immigration Data Repository System of Records Notice (SORN) continues to provide coverage for the CIDR system.[11] Furthermore, the following SORNs provide coverage for CIDR receiving data from CLAIMS 3, planned future data sets,[12] and other USCIS systems:

- Benefits Information System,[13] covers USCIS's collection, use, maintenance, dissemination, and storage of benefit request information, including case processing and decisional data not included in the Alien File;
- Asylum Information and Pre-Screening,[14] covers the collection and use of affirmative asylum applications,[15] applications filed with USCIS for suspension of deportation, special rule cancellation of removal pursuant to the Nicaraguan Adjustment and Central American Relief Act,[16] credible fear screening cases,[17] and reasonable fear[18] screening cases;
- Refugee Case Processing and Security Screening Information,[19] covers the collection and use of data relating to refugee applicants, refugee derivatives, and follow-to-join applicants;

[11] DHS/USCIS-012 Citizenship and Immigration Data Repository (CIDR), 83 FR 19082 (May 1, 2018).
[12] As USCIS adds data sets to CIDR, they will be added to Appendix A. The Appendix will also be updated to include any new SORNs.
[13] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[14] DHS/USCIS-010 Asylum Information and Pre-Screening, 80 FR 74781 (Nov. 30, 2015).
[15] USCIS, through its Asylum Division, administers the affirmative asylum program to provide protection to qualified individuals in the United States who have suffered past persecution or have a well-founded fear of future persecution in their country of origin, as outlined under Section 208 of the Immigration and Nationality Act (INA), 8 U.S.C. § 1158 and 8 CFR Part 208. To obtain asylum, the individual must be physically present in the United States. Generally, an individual may apply for affirmative asylum status regardless of how he or she arrived in the United States or his or her current immigration status.
[16] *See* Nicaraguan Adjustment and Central American Relief Act, Pub. L. No. 105-100, § 203, 111 Stat. 2193, 2196-200 (1997).
[17] *See* 8 U.S.C. § 1225(b)(1)(B).
[18] *See* 8 CFR Part 208.31.
[19] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075

- Alien File, Index, and National File Tracking System,[20] covers the paper and electronic copy Alien File and/or Receipt File, supplemental forms, supplemental evidence, and identity history summaries (formally known as the Record of Arrest and Prosecution Sheet (RAP sheets)), but does not include all case processing and decisional data;
- Fraud Detection and National Security Records,[21] covers FDNS's general collection, use, maintenance, and sharing of records for fraud, public safety, national security, and intelligence purposes.
- Internal Affairs System of Records[22] covers OSI's access and use of source system audit logs.

CIDR received a final Authority to Operate (ATO) May 11, 2017, and is subject to renewal every three years.

USCIS is continuing to draft a CIDR retention schedule. USCIS is proposing to retain audit logs, record searches, and reports for at least five years, but not more than 25 years, after the last interaction with the individual. USCIS proposes to retain a record of the classified search request, the results of the request for a minimum of five years, in accordance with Director of Central Intelligence Directive (DCID) 6/3, and up to 25 years. Finally, USCIS is proposing to retain classified background check results from immigration requests for 100 years from the subject's date of birth. CIDR does not retain the replicated data sets from the underlying USCIS data systems. Data supplied by these systems are retained in the source system in accordance with their respective retention schedules. Records used as part of a benefit determination will be maintained in the paper or electronic Alien File and processed in the respective USCIS case management system. USCIS transfers Alien Files to the custody of the National Archives and Records Administration (NARA) 100 years after the individual's date of birth.

This update does not impact the Paperwork Reduction Act (PRA) section in DHS/USCIS/PIA-031(a). While there are no forms directly associated with CIDR, the information within CIDR may originally be derived from USCIS applications that are covered by the PRA. Further detail on how these various forms cover the initial collection of information from the individual and how they are used may be found in the Benefit Request Intake Process PIA.[23]

(Oct. 19, 2016).

[20] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sep. 18, 2017). The Alien File, Index, and National File Tracking System of Records is the official record system that contains information regarding the transactions of an individual as he/she passes through the U.S. immigration and inspection process. It may also contain information related to U.S. born citizens and others involved in certain immigration crimes. Final Rule for Privacy Act Exemptions, 78 FR 69983 (Nov. 22, 2013).

[21] DHS/USCIS-006 Fraud Detection and National Security, 77 FR 47411 (Aug. 8, 2012).

[22] DHS/ALL-020 Internal Affairs System of Records, 79 FR 23361, (April 28, 2014).

[23] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy. See Appendix A of

Characterization of the Information

Data Sources (Systems)

CIDR was developed to be able to replicate data from the USCIS IT systems used to process immigrant and nonimmigrant applications and petitions or other immigration requests. CIDR now uses eCISCOR[24] as its primary data source to access CLAIMS 3 data and to access planned future data sets. eCISCOR stores incrementally updated copies of transactional source systems' data for use by DHS end-users for reporting, analytic, and data sharing purposes. eCISCOR accesses source system information and translates it from the source system format to an eCISCOR readable format for consumption by other USCIS source systems. USCIS is relying on extracting immigration request data via eCISCOR, rather than directly from the source systems, which reduces disruptions to the source systems.

The process for transferring data from the unclassified to the classified network remains unchanged from the January 2017 PIA. USCIS controls what and when data is transferred by placing it into a file drop zone on the unclassified domain. The CDS then extracts the data, validates, scans, and transfers it to a file drop zone in the classified domain.

As for the remaining data sources planned to be ingested into CIDR, many of the systems identified as data sources in the January 2017 PIA have been updated or replaced as part of a recent IT modernization effort. For example, USCIS now process many immigrant and non-immigration applications and petitions in USCIS Electronic Immigration System (USCIS ELIS)[25] rather than CLAIMS 4,[26] which is planned to be decommissioned, and Global,[27] rather than RAPS/APSS,[28] which has been retired. As USCIS adds the planned future data sets to CIDR, the source system and its data sets will be added to Appendix A.

Expansion of Retrievable Data Elements

CIDR maintains limited information on the users of the underlying systems through audit logs that OSI uses to discover linkages in which an employee, either for personal gain or by

---

that PIA for specific forms and associated OMB Control Numbers.

[24] *See* DHS/USCIS/PIA-023(b) eCISCOR, *available at* www.dhs.gov/privacy.

[25] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available at* www.dhs.gov/privacy.

[26] CLAIMS 4 is an electronic case management application tracking and processing system used as automated support for the variety of tasks associated with processing and adjudicating N-400, *Applications for Naturalization*. For more information, *see* DHS/USCIS/PIA-015 Computer Linked Application Information Management System 4 (CLAIMS 4) Update, *available at* www.dhs.gov/privacy.

[27] *See* DHS/USCIS/PIA-027 Asylum Division, *available at* www.dhs.gov/privacy.

[28] RAPS is used to verify the status of asylum applicants, asylees, and their dependents, to assist with the verification of an individual's immigration history in the course of a review of visa petitions and other benefit applications as well. APSS supports USCIS in the screening of individuals in the expedited removal process and of individuals subject to reinstatement of a final order of removal or an administrative removal order based on a conviction of an aggravated felony to determine whether they have credible fear or reasonable fear. For more information, *see* DHS/USCIS/PIA-027 Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) Update, *available at* www.dhs.gov/privacy.

coercion, may be attempting to manipulate the immigration system. Identification of such linkages using data from CIDR allows OSI to identify appropriate internal control mechanisms to put in place to prevent these actions – mechanisms that can be tested annually. Previously, these records were retrievable by a PICS ID. The expanded data elements are not new data elements. Rather, they are existing source system data elements that may now be used to retrieve information within the audit logs since the PICS ID is no longer used throughout the Department. USCIS is updating this PIA to reflect additional data fields that are searchable/retrievable in CIDR, related to the adjudicator, including:

- Adjudicator/User ID;
- Last Name;
- First Name;
- Title;
- Location;
- First Line Supervisor; and
- Field Office Director.

All other data elements are unchanged from the January 2017 PIA. Because CLAIMS 3 is the only data set ingested into CIDR as of publication of this PIA, the data elements are reflective of those available to CIDR from the underlying data available in CLAIMS 3. Should the data elements change when future data sets are ingested into CIDR, USCIS will update PIA Appendix A, documenting the source system and corresponding data elements from the respective system. USCIS will continually update this Appendix as more source systems are ingested and new data elements outside what was previously captured in DHS/USCIS/PIA-031(a) and this PIA Update are added.

Privacy Risk: There is a risk that the data that eCISCOR sends to CIDR is inaccurate and untimely.

Mitigation: This risk is partially mitigated. eCISCOR depends on the accuracy and quality of information provided by the source systems. Data maintained in eCISCOR is frequently updated to capture data changes. This process reduces the risk of data discrepancies between eCISCOR and the source systems. In addition, eCISCOR access is limited to read-only connectivity, to preserve the integrity and accuracy of the information derived from USCIS source systems.

Uses of the Information

Fraud Detection and National Security Directorate (FDNS)

FDNS's use of CIDR remains unchanged from DHS/USCIS/PIA-031(a) issued January 2017. FDNS continues to use CIDR to enhance USCIS' vetting capabilities and respond to RFIs involving classified information.

Office of Security and Integrity (OSI)

OSI's use of CIDR remains unchanged from DHS/USCIS/PIA-031(a) issued January 2017. OSI continues to use CIDR in support of its mission, which includes analyzing existing data sets from internal sources to identify anomalies that could indicate insider corruption or fraud. However, USCIS previously identified the PIB as a user of CIDR. Due to organizational changes within OSI, PIB is no longer being referenced as the sole user. Instead, USCIS is updating this PIA to state that information from CIDR will be used by OSI in support of fulfilling the statutory requirements of Section 453 of the Homeland Security Act.

Notice

This update does not impact the notice to individuals. USCIS is providing general notice through this PIA update and the CIDR SORN.

Data Retention by the project

This update does not impact the retention of information in CIDR. USCIS is drafting a CIDR retention schedule. USCIS is proposing to retain audit logs, record searches, and reports for at least five years, but not more than 25 years, after the last interaction with the individual. USCIS proposes to retain a record of the classified search request, the results of the request for a minimum of five years, in accordance with Director of Central Intelligence Directive (DCID) 6/3, and up to 25 years. Finally, USCIS is proposing to retain classified background check results from immigration requests for 100 years from the subject's date of birth. CIDR does not retain the replicated data sets from the underlying USCIS data systems. Data supplied by these systems are retained in the source system in accordance with their respective retention schedules. Records used as part of a benefit determination will be maintained in the Alien File and processed in the respective USCIS case management system. USCIS transfers Alien Files to the custody of NARA 100 years after the individual's date of birth.

Privacy Risk: CIDR does not have a NARA-approved records retention schedule, which could result in records being retained for longer than necessary.

Mitigation: This risk is partially mitigated. USCIS is developing a retention schedule for CIDR and will not delete records until a retention schedule is approved by NARA. USCIS plans to propose a NARA schedule that is to be consistent with the concept of retaining data only for as long as necessary to support USCIS mission. Until USCIS completes a NARA-approved retention

schedule, USCIS plans to maintain all records indefinitely in accordance with the Federal Records Act, which prohibits agencies from destroying records without a NARA-approved schedule.

Information Sharing

This update does not impact the external sharing in CIDR. USCIS continues to share information outlined in Section 6.0 of the DHS/USCIS/PIA-031(a) Citizenship and Immigration Data Repository PIA, published in January 2017.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. DHS exempted CIDR records from general access provisions pursuant to 5 U.S.C. § 552a(k)(l) and (2). USCIS reviews each request for information within CIDR to determine whether or not the record within CIDR meets the requirements of the exemptions and, as appropriate, disclose information that does not meet the requirements. This does not prevent the individual from gaining access to his or her records that are found within the original source system. Persons may seek access to records maintained in the source systems that feed into CIDR.

USCIS continues to provide individuals with access to their information through Privacy Act or Freedom of Information Act (FOIA) requests. 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

There is no change to CIDR's auditing and accountability procedures. USCIS continues to follow the requirements of the DHS 4300A Sensitive Systems Handbook for information assurance and security and employs access controls and an aggressive auditing strategy that goes above and beyond the requirements of DCID 6/3, section 4.B.2.a(4), to ensure the data is secure, and the system is used for the stated purposes.

Responsible Official

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

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

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

APPENDIX A

USCIS Source System Data Sets Received via eCISCOR

Source System	PIA	SORN
CLAIMS 3	DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems	• DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System • DHS/USCIS-018 Immigration Biometric and Background Check • DHS/USCIS-007 Benefits Information System