Privacy Impact Assessment
for the

Enterprise Gateway and Integration Services (EGIS)

DHS/USCIS/PIA-080

June 28, 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) is migrating its information technology systems to the cloud environment to align with the Cloud Smart initiative. To support this modernization effort, USCIS launched the Enterprise Gateway and Integration Services (EGIS) to connect and share data from different systems. EGIS acts as a conduit for the exchange of information between systems within USCIS, the Department of Homeland Security (DHS), external government agencies, and authorized third parties. EGIS is designed to replace the Enterprise Service Bus 2 (ESB 2) and its hosted services incrementally. Until the ESB 2 hosted services are fully integrated into EGIS, USCIS plans to maintain legacy ESB 2 as there is a continued need to sustain the exchange of information between legacy operational systems. EGIS will also consolidate some ESB 2 functionality and add functionality not found in ESB 2 (e.g., Payment Validation Services). USCIS plans to update and publish this Privacy Impact Assessment (PIA) in a phased approach to evaluate the privacy risks and mitigations associated with the collection, use, and dissemination of personally identifiable information (PII) by the migrated and new services hosted by EGIS.

Overview

USCIS oversees lawful immigration to the United States. USCIS is responsible for processing petitions, applications, and other immigration-related requests. To fulfill its mission, USCIS may share information with, or receive information from other USCIS, DHS, and non-DHS systems. USCIS uses systems that were implemented at different points in time for different purposes using a variety of underlying technology infrastructures (including legacy mainframe database systems, Oracle-based server systems, and newer service-oriented systems), but all of these various systems are required to communicate with each other.

USCIS is undergoing a system modernization effort to align with the Cloud Smart initiative.[1] Cloud Smart is a new strategy for agencies to adopt cloud solutions that streamline transformation and embrace modern capabilities. To support this modernization effort, USCIS is shifting its use of the ESB 2 to the EGIS to connect and share data from different operating systems. [2]

Serving as a conduit, EGIS continues to act as an intermediary service orchestrating the connection between applications, so that all data exchanges take place through EGIS. Similar to ESB 2, EGIS assists with the seamless and accurate exchange of information from different systems by facilitating the transfer of data. The transfer of information is invoked by the end source systems. When exchanging data from one system to another, EGIS formats the message from one

[1] *See* https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[2] *See* DHS/USCIS/PIA-008(a), Enterprise Service Bus 2, *available at* www.dhs.gov/privacy.

system to another format to enable effective and secure synchronization and integration of data. To achieve system interoperability, both systems must refer to a common information exchange reference model. As a backend system, EGIS reconciles different operating systems and standards in order to address interoperability complexities and challenges. EGIS does not retain any operational information.

EGIS serves as the foundation infrastructure that hosts and supports USCIS business services and provides the service-oriented architecture platform for USCIS. EGIS enables real-time information sharing between enterprise applications within USCIS, DHS, external government agencies, and other authorized partners with little or no modifications needed to the systems being integrated. USCIS EGIS facilitates data synchronization and integration of the following services:

- **Adoption Case Management System (ACMS) Orchestration Services (AOS)** facilitates communication between the USCIS ACMS[3] and to the Department of State (DOS) Consular Consolidated Database (CCD).[4]
- **Lockbox Intake Service (LIS)** facilitates communication between the Lockbox[5] to the respective USCIS case management systems (e.g., Computer Linked Application Information Management System (CLAIMS 3),[6] Global,[7] and INFACT[8]) for initial benefit forms.
- **Refugee Asylum Support Service (RASS)** facilitates the refugee vetting through the automated sharing of information between the DOS, U.S. Customs and Border Protection (CBP), USCIS, and other vetting agencies.[9] RASS interfaces with DOS Worldwide Refugee Admissions Processing System (WRAPS)[10] for ingestion into the Case and Activity Management for International Operations (CAMINO).[11] USCIS

[3] *See* DHS/USCIS/PIA-007(b) Domestically Filed Inter-country Adoptions Applications and Petitions, *available at* www.dhs.gov/privacy.
[4] *See* DOS Consular Consolidated Database (CCD) PIA, *available at* https://www.state.gov/documents/organization/242316.pdf.
[5] Lockbox is a facility, operated by the Department of Treasury, which allows USCIS to receive benefit request forms more quickly and process fee payments more efficiently and securely.
[6] *See* DHS/USCIS/PIA-016 Computer Linked Application Information Management System and Associated Systems (CLAIMS 3), *available at* www.dhs.gov/privacy.
[7] *See* DHS/USCIS/PIA-027 Asylum Division, *available at* www.dhs.gov/privacy.
[8] *See* forthcoming EB-5 Program PIA, which will be *available at* www.dhs.gov/privacy.
[9] *See* DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting, *available at* www.dhs.gov/privacy.
[10] WRAPS is the DOS case management database used for all refugee applicants processed for resettlement consideration to the United States. For more information, see the WRAPS PIA and SORN, available at https://2001-2009.state.gov/documents/organization/101146.pdf. Refugee Processing Center (RPC), operated by DOS contractors, is the central data repository for all overseas and domestic resettlement operations. The RPC manages the WRAPS database.
[11] *See* DHS/USCIS/PIA-051 Case and Activity Management for International Operations (CAMINO), *available at* www.dhs.gov/privacy.

RASS also passes the refugee information derived from WRAPS to CBP's Automated Targeting System (ATS).[12] ATS, in turn, transmits data to partner agencies in the law enforcement and intelligence community, such as National Counter Terrorism Center (NCTC).

- **USCIS Visa Support Services (VSS)** is a service that collects biometrics and limited biographic information from participating USCIS Application Support Centers (ASC) on behalf of several countries that require biometric and biographic data as part of their visa issuance process for visitors to their respective countries.[13]

These services were previously supported by legacy ESB but are being absorbed into EGIS. Until all of the ESB 2 services are fully integrated into EGIS, USCIS plans to maintain legacy ESB 2 as there is a continued need to sustain the exchange of information between legacy operational systems. USCIS plans to incrementally migrate the remaining services from ESB 2 to EGIS. USCIS may also integrate new services into EGIS.[14] USCIS plans to update and reissue this PIA and the ESB 2 PIA[15] as services are shifted from ESB 2 to EGIS, or new services are added to the EGIS infrastructure. USCIS plans to retire the ESB 2 PIA when ESB 2 is full dispositioned.

EGIS contains a set of common services, which include auditing, error handling, authentication services, payment validation, document format conversion, and encryption services. EGIS enables USCIS to implement greater security and privacy measures into the data usage and transfer process by providing a centralized mechanism for authenticating and authorizing system access. EGIS employs auditing measures to prevent inappropriate dissemination of data and facilitate incident forensics, which is the collection and examination of digital evidence residing on electronic systems and the subsequent response to threats and attacks. DHS security specifications require auditing capabilities that log the activity of each transaction in order to reduce the possibility of inappropriate dissemination of information.

[12] *See* DHS/CBP/PIA-006(e) Automated Targeting System, *available at* www.dhs.gov/privacy.
[13] *See* DHS/USCIS/PIA-048(a) USCIS International Biometric Processing Services, *available at* www.dhs.gov/privacy.
[14] Please see the Appendices to this PIA for more information regarding the collection, use, storage, and dissemination of information between different systems.
[15] *See* DHS/USCIS/PIA-010(a) Enterprise Service Bus, *available at* www.dhs.gov/privacy.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

USCIS collects and uses information under the authority of the Immigration and Nationality Act (INA).[16] Specifically, 8 U.S.C. § 1103 charges the Secretary of Homeland Security with the duty of administering and enforcing all laws relating to the immigration and naturalization of aliens.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EGIS is the foundational infrastructure that enables real-time information sharing between enterprise applications within USCIS, DHS, external government agencies, and authorized organizations. The source system SORNs described in the attached Appendices cover the collection, use, maintenance, and dissemination of information by the subsystem services.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. EGIS is a major application and includes integrated subsystems within its accreditation boundary. The EGIS Authority to Operate (ATO) is pending the publication of this PIA. EGIS will enter into the Ongoing Authorization (OA) program upon completion of this PIA. OA requires EGIS to be reviewed by the USCIS OA Team on a monthly basis and maintain its security and privacy posture to maintain its ATO.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. EGIS does not retain any operational information from a query. EGIS transmits data and immediately deletes all information after the information is sent to the receiving system. Thus, EGIS does not require a NARA-approved records retention schedule. However, the systems from which EGIS transmits information may have NARA-approved retention schedules. Please see the Appendices for source system retention schedules.

[16] *See* 8 U.S.C. § 1101 et seq.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No. The provisions of the PRA do not apply to EGIS.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

EGIS is an intermediary system, meaning that it connects different source systems together to enable communication among them. EGIS hosts several connecting services that each serve as a separate messenger to the receiving system. Each service transforms the message into a format that the receiving system is able to interpret and ingest. EGIS does not maintain or store any operational data once the information is transmitted. Usually data is in queue until it is processed. Please see the Appendices of this PIA for a complete list of data elements transmitted and exchanged by each EGIS service.

2.2 What are the sources of the information and how is the information collected for the project?

EGIS is an intermediary system facilitating communications between different systems. Please see the Appendices of this PIA for a complete list of sources of information for each EGIS service.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. EGIS does not itself maintain or use this type of information. However, the information that EGIS transmits from one source system to another may contain information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

EGIS depends on the accuracy and quality of information from each source system. EGIS ensures the accuracy of the data by collecting the information directly from the source systems. For data that may be transferred through EGIS, the data is queried from the underlying systems and is delivered “as is” with the exception of reformatting to standardize the representation of the data. Any checks for accuracy of the data are accomplished at the originating site, and are out of

scope of EGIS or the services that EGIS controls. EGIS cannot and does not provide any assurance that the data it delivers is accurate; it simply transports the data from one format to another.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of exposing personal information in audit data.

Mitigation: EGIS mitigates this risk by not retaining operational data in the audit log files. Auditing is a fundamental security principle that provides the ability to track the activities of a user or system that may access information maintained within a system. Audit trails track the identity of each subject attempting to access a system, the time and date of access, and the time of log off. Data in the audit log files contain general transactional information that is helpful in identifying the transaction and user.

Privacy Risk: There is a risk that inaccurate information is transferred to the receiving systems from the EGIS services.

Mitigation: This risk cannot be not fully mitigated. EGIS depends on the accuracy and quality of information from each source system. EGIS does not change data from the source system "en route" to the receiving system other than to provide standardized formatting of the data, such as date and time formatting. Furthermore, USCIS leverages technology tools that allow for streaming services, including data filtering, to investigate and understand the data based on need-to-know basis for specific systems.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The purpose of EGIS is to support the integration of legacy and different operating systems. The EGIS services enable the seamless integration, communication, and exchange of data between systems. Please see the Appendices of this PIA, which describe how and why the EGIS services may transfer information. Additionally, the associated source system and program PIAs also describe the data transport, system connection, or information access for a particular EGIS hosted service.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that improper identity and access controls may expose information to malicious or un-authorized users.

Mitigation: EGIS mitigates this risk by protecting the data for role-based access control of services controlled and managed by the EGIS with encryption and access control. Only EGIS administrators will have access to this data and the most critical portion of this data, the password, is stored using irreversible encryption.

The data delivered by the EGIS is protected by numerous security controls. The security controls of EGIS ensure that the data from the underlying connected systems remains intact from when it is first queried from the original underlying source system until it is delivered to the consuming application or end user. The primary method of this control is the use of secure socket layer (SSL) processing between all components that do not reside on the same physical machine. SSL processing ensures that data may not be altered during communications. The SSL mechanisms involved are all Federal Information Processing Standard 140-2 compliant per DHS policy.

EGIS audit logs will only be reviewed if there is suspicious activity that leads to a need to review. The EGIS audit review is performed by USCIS IT Security if they determine that there is suspicious activity or that there may have been a security breach. Any reconstruction of events is a manual process performed by IT Security. The audit logs are only accessible to IT Security upon request, and EGIS administrators only for archival and storage management purposes.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

EGIS does not collect information directly from individuals. USCIS provides general notice to individuals through a Privacy Notice on all USCIS forms' instructions, which are the original point of collection. This PIA, associated source system PIAs, and SORNs listed in the Appendices to this PIA also provide notice.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

EGIS does not collect information directly from individuals. USCIS provides applicants seeking USCIS benefits with a Privacy Notice contained on all benefit request form instructions. The Privacy Notice details the authority for the collection of the information requested and the uses of information. As a general rule, USCIS provides notice that the information collection is voluntary, and that the individual may decline to provide the requested information. However, failure to provide the requested information may delay a final decision or result in the denial of the applicant's immigration request. On each immigration request form, USCIS includes a release authorization statement that requests the applicant's signature to permit USCIS to release any information from the applicant's records necessary to determine eligibility for the requested benefit.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Because EGIS is not the source system of collection, there is a risk that individuals will not receive notice of the purpose for which EGIS uses their information.

Mitigation: While this risk is not fully mitigated, USCIS has taken a number of steps to provide notice of EGIS. First, USCIS provides the individual with a Privacy Notice explaining the purpose of collection at the original point of collection, and through those corresponding source system PIAs and applicable SORNs. Second, notice of source system interactions with EGIS is provided through the publication of this PIA.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

EGIS does not save data from any of the systems that are connecting through EGIS. EGIS does not maintain/retain any data once the data is exchanged. Usually, the data is retained in memory (queue) only for a few seconds for processing; however, EGIS queues may retain data for up to seven days to ensure the successful delivery of data to the receiving system from the source system. Data in the queue will be encrypted at rest. Once the data is delivered, the information no longer resides in EGIS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: EGIS transmission queues may retain transmitted data for retransmission or transmission transaction recovery.

Mitigation: This risk is partially mitigated. All information being transported in EGIS queues are encrypted at rest There is no risk related to retention of data because EGIS does not

save data, it simply transports data from one system to another. EGIS queues may retain data for up to seven days to ensure the successful delivery of data to the receiving system from the source system. Data in the queue will be encrypted at rest. Once the data is delivered, the information no longer resides in EGIS.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

EGIS facilitates information sharing with federal, state, local, and foreign government agencies and authorized organizations in accordance with approved routine uses, as described in the source system's associated published SORNs. The EGIS services may share USCIS information and records with outside entities, either pursuant to regulation or through specific agreements. EGIS supports the exchange of information with the following external entities:

Department of State (DoS)

EGIS shares information from USCIS with DOS for the purpose of processing applications and petitions under the INA. ACMS-AOS and RASS facilitate the sharing of benefit requestor information with DOS. AOS transmits intercountry adoption data to DOS CCD.[17] RASS retrieves refugee case information from DOS WRAPS.[18]

International Partner Agencies

USCIS ASCs collect applicant biometric and biographic information on behalf of international partner governmental agencies. VSS transmits the individual's information to the partner agencies.[19] Please see the Appendices of this PIA to learn more about the External Sharing practices of each EGIS service.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Before transferring information, USCIS verifies that the sharing is for a purpose compatible with the original purpose for which USCIS collected the information.

Department of State

[17] *See* DOS CCD PIA (July 17, 2015), available at https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.
[18] *See* https://2001-2009.state.gov/documents/organization/101146.pdf.
[19] *See* DHS/USCIS/PIA-048 USCIS International Biometric Processing Services, *available at* www.dhs.gov/privacy.

Sharing USCIS data with DOS is compatible with the purpose of the system because the DOS mission, like USCIS, includes ensuring visits and immigration to the United States are lawful as dictated by the INA. USCIS shares information with DOS as permitted under the following routine uses:

- Routine Use I in DHS/USCIS-005 Intercountry Adoptions permits information sharing with the DOS in the processing of petitions or applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements.[20]
- Routine Use H of DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records permits the sharing of information with the DOS when necessary to accomplish refugee case processing.[21]

International Partner Agencies

USCIS temporarily retains information collected on behalf of a partner country for only as long as it takes to successfully transmit the information to the partner country. While temporarily retained, USCIS does not retrieve the records using a unique personal identifier. USCIS transfers the biographic information and biometric capture to the partner country immediately after collection. USCIS deletes the information from EGIS after the partner country provides confirmation of the successful transfer of the information. Therefore, no SORN is required to cover this collection.

6.3 Does the project place limitations on re-dissemination?

Yes. A Memorandum of Understanding/Agreement (MOU/A) exists between DHS and all recipient external organizations that places limitations on re-dissemination of information. External organizations may only share information under the MOU when the recipient has an official need, in accordance with the terms of the MOU/A, and allowed by applicable privacy and confidentiality statutes. Additionally, the MOU/A clarifies the authority for external organizations and DHS to share immigration and naturalization records and the basic mechanisms established to protect this data.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

EGIS services shares information with external systems and maintains audit and transactional logs of all data sent through EGIS.

[20] DHS/USCIS-005 Intercountry Adoptions, 81 FR 78614 (Nov. 8, 2016).
[21] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that USCIS may potentially disclose data for a purpose that is not compatible with the original purpose for collection.

Mitigation: USCIS mitigates this risk by ensuring the information sharing is compatible with the purpose for collection prior to disclosing any information. USCIS reviews the routine uses in the applicable SORNs to verify the compatibility of an information exchange prior to disclosing data. DHS has MOU/As in place with external agencies to ensure that there are formal procedures in place to secure and protect biographic and biometric information. The agreements between DHS and external entities fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. As discussed above, EGIS maintains a record of disclosure of information in accordance with the associated routine use or information sharing agreement. Records are kept as system audit trail logs, which are maintained to identify transactions performed by users. In addition, USCIS ensures through the MOU/A process that the external agencies have policies, procedures, and training in place to ensure that information is not inappropriately disseminated.

Privacy Risk: There is a risk that data shared externally from a source system via EGIS may be inaccurate.

Mitigation: This risk cannot be fully mitigated. EGIS depends on the accuracy and quality of information from each source system. EGIS ensures the accuracy of the data by collecting the information directly from the source systems. For data that may be transferred through EGIS, the data is queried from the underlying systems and is delivered "as is" with the exception of reformatting to standardize the representation of the data.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

EGIS does not store any records. However, an individual may seek access to his or her USCIS records in a source system by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Account holders 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. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

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

Some information requested may be exempt from disclosure under the Privacy Act or FOIA because information may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations. Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

EGIS does not employ any mechanisms that allow individuals to amend erroneous information. EGIS maintains read-only data, for a short amount of time, obtained from the source systems, and USCIS personnel cannot amend EGIS records directly. EGIS has a refresh mechanism that updates on a regular basis to reflect any changes in the source systems records; this refresh helps ensure timely and accurate data.

While EGIS does not permit individuals to correct inaccurate or erroneous information itself, U.S. citizens, lawful permanent residents, and other persons with records covered by the JRA are afforded the ability to correct information within source systems and interconnected systems by filing a Privacy Act Amendment request under the Privacy Act. U.S. citizens, lawful permanent residents, and persons covered by the JRA should submit requests to contest or amend information contained in the source system as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, the proposed amendment, and any evidence of the correct information. The record must be identified in the same manner as described for making a request for access. If the request is accepted, any amendment would only apply to USCIS-held information. Persons not covered by the Privacy Act are not able to amend their records through FOIA. If non-U.S. persons find inaccurate information in their records received through FOIA, they may visit a local USCIS Field Office to identify and amend inaccurate records with evidence supporting their reasons for amendment.

7.3 How does the project notify individuals about the procedures for correcting their information?

EGIS does not employ mechanisms or procedures to notify individuals on how to amend their information that may be contained within the source system. EGIS transports data between USCIS systems, other DHS systems, and external systems. The SORNs and PIAs for the source systems explain how individuals can correct erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk associated with redress. EGIS does not store any records. Any redress mechanisms would come from the source system.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ensures that practices stated in this PIA comply with federal, DHS, and USCIS standards, policies, and procedures, including standard operating procedures, rules of behavior, and auditing and accountability procedures. EGIS is maintained in the Amazon Web Services (AWS), which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines. AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[22] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.[23]

USCIS requires EGIS to undergo the security assessment process to verify adherence to DHS privacy and security requirements. USCIS validates technical and security controls to preserve the confidentiality, integrity, and availability of the data during the security authorization process. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further, DHS security specifications 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.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All USCIS employees and contractors are required to complete annual privacy awareness and computer security awareness training to ensure their understanding of properly handling and securing PII. The privacy awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs). The computer security awareness training examines

[22] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. More information available at https://www.fedramp.gov/.
[23] *See* https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.

appropriate technical, physical, personnel, and administrative controls to safeguard information. USCIS also provides role-based training on the proper uses of USCIS information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

USCIS only grants back-end access to EGIS to authorized personnel (administrator role only) on a strictly need-to-know basis. USCIS audits user access in accordance with the DHS Sensitive Systems Policy Directive, which requires 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.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS has a formal review and approval process in place for new sharing agreements. Any new use of information and/or new access requests for the system must go through the USCIS change control process and must be approved by the proper authorities of this process, such as the DHS Headquarters (including Office of General Counsel, Civil Rights and Civil Liberties, Office of Intelligence and Analysis, and the Privacy Office), USCIS Privacy Officer, Chief of Information Security Officer, Office of the Chief Counsel, and the respective Program Office.

8.5 Privacy Impact Analysis: Related to the Accountability and Integrity of the Information

Privacy Risk: The data maintained by AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with EGIS, whether on a USCIS infrastructure or on a vendor's infrastructure and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[24]

Responsible Officials

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

[24] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

APPENDIX A

Adoption Orchestration Services (AOS)

Background:

Adoption Orchestration Services (AOS) facilitates the secure connection between the USCIS Adoption Case Management System (ACMS)[25] and the DOS CCD in support of inter-country adoptions.[26] USCIS adjudicators are able to electronically share intercountry adoption filings from ACMS to CCD through AOS. AOS reads the message from ACMS, transforms the data using the mappings defined in the AOS, and updates DOS CCD in a compatible format.

Information Collected, Retained, and Disseminated and Source(s) of any PII and SPII:

The intercountry adoption information shared with DOS includes information captured on the intercountry adoption forms, supporting evidence, the home study, all Requests for Evidence (RFE), background check results, and approval and denial notices.

Category of Individuals Affected:

Intercountry Adoption filings include information on the prospective adoptive parents, children household members, adult household members, and adoptive beneficiaries.

Information Sharing:

AOS facilitates the secure connection between USCIS ACMS and the DOS CCD.

Applicable System of Records Notice:

The Intercountry Adoptions SORN covers the information collected during the intercountry adoptions process and sharing of information with DOS.[27]

Retention:

AOS does not maintain/retain any data. The data is temporarily in queue for processing, which is usually no longer than a few seconds

[25] S*ee* DHS/USCIS/PIA-007(b) Domestically Filed Intercountry Adoptions Applications and Petitions, *available at* www.dhs.gov/privacy.
[26] *See* DOS CCD PIA (July 17, 2015), *available at* https://foia.state.gov/_docs/pia/consularconsolidateddatabase_ccd.pdf.
[27] *See* DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016).

APPENDIX B

Lockbox Intake Service (LIS)

Background:

Lockbox facilities are operated by a specialized contractor authorized by the Department of Treasury (Treasury). This contractor manages the intake of USCIS immigration and non-immigrant requests and the collection of associated fees submitted directly by mail. It provides the mechanisms to capture information electronically from USCIS benefit request forms, deposit associated fees, move the information to USCIS systems via a system interface, and generate acceptance and rejection notices to immigration requestors. The contractor is also responsible for preparing the application-related files in accordance with USCIS guidance and sending the files to the next processing site (i.e., Service Center). The contractor does not approve or deny benefit request forms received by the USCIS Lockbox.

The Lockbox is the primary data entry point for the intake of immigrant and non-immigrant filings. The forms are scanned and electronically parsed and then picked up by the LIS. The service accepts data representing the benefit request forms as well as the receipting and remittance data for the benefit request forms. LIS then distributes this data to the appropriate USCIS case management system.[28]

Information Collected, Retained, and Disseminated and Source(s) of any PII and SPII:

The Lockbox scans an image of the immigration and non-immigrant request form and supporting documentation into an electronic format. Lockbox personnel perform data entry on an as needed basis for forms that do not convert properly in electronic format. Lockbox personnel compare the physical benefit request form and payment against the data in electronic format and make corrections as needed. Once the physical form is converted into electronic format, it is sent to the appropriate case management system. Files are transmitted via the LIS and are also ingested into the Enterprise Document Management System (EDMS) Receipt File Repository.[29]

Category of Individuals Affected:

The information collected as part of the benefit request intake and receipt process is provided by the benefit requestor, accredited representative, form preparer, or interpreter on the completed benefit request form and from supplemental documentation.

Information Sharing:

[28] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.
[29] EDMS is a web-based system that allows authorized users to view and search electronic copies of the paper-based case files: A-Files and Receipt Files. *See* DHS/USCIS/PIA-003 - Integrated Digitization Document Management Program, *available at* www.dhs.gov/privacy.

USCIS LIS receives immigration applications and petitions along with supporting documents from the JP Morgan Chase (JPMC) Lockbox Service Provider via EGIS. The application data is transmitted to USCIS backend systems (CLAIMS 3,[30] Global,[31] and USCIS Electronic Immigration System.[32])

Applicable System of Records Notice:

The following SORNs cover the collection, maintenance, and use of the information of the benefit request intake and receipt process:

- Alien File, Index, and National File Tracking System, which covers the collection, use, and maintenance of benefit requests forms and supplemental evidence;[33] and
- Benefits Information System, which covers the collection and use of immigrant and nonimmigrant benefit request forms, decisional data, and associated fees for adjudication.[34]

Retention:

LIS service does not maintain/retain any data. The data is temporarily in queue for processing, which is usually no longer than a few seconds. Once successfully or unsuccessfully processed, the data is no longer available in LIS.

[30] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.
[31] *See* DHS/USCIS/PIA-027(c) Asylum Division, *available at* www.dhs.gov/privacy.
[32] *See* DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), *available at* www.dhs.gov/privacy.
[33] *See* DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[34] *See* DHS-USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).

APPENDIX C

EGIS Refugee Asylum Support Service (RASS)

Background:

Pursuant to various information sharing documents, DHS, DOS, and several vetting agencies in the law enforcement and intelligence community have developed a process to share refugee application data in DOS's Worldwide Refugee Admissions Processing System (WRAPS)[35] to enable vetting of DOS WRAPS data against each agency's respective holdings to identify possible derogatory information related to individuals seeking refugee status. EGIS RASS is used as a vehicle to receive and transmit application data to partner agencies in the law enforcement and intelligence community.

DOS provides the applicant's information via DOS WRAPS to USCIS through the EGIS RASS and for ingestion into the Case and Activity Management for International Operations (CAMINO).[36] USCIS RASS also passes the DOS WRAPS information to CBP ATS.[37] ATS serves as a technical pass through, providing the information to National Counter Terrorism Center (NCTC), which may result in a match to derogatory holdings, when it exists. Any information that is returned by ATS is sent to CAMINO, which is then used by USCIS personnel to compile and provide a final response to DOS WRAPS. The responses are considered by DOS for determination regarding issuance of a visa and by USCIS for its determination on whether to grant the benefit.

Information Collected, Retained, and Disseminated and Source(s) of any PII and SPII:

DOS enters applicant information it has received into WRAPS to be forwarded to vetting partners, including NCTC. The documents include information about the applicants, as well as about family members and other associates. The information relating to applicants includes: name, date of birth, city and country of birth, height, weight, gender, addresses, phone numbers, employment information, and identity documents. The information relating to family members and associates includes: name, date of birth, country of birth, gender, addresses, and phone numbers. This information is ingested into CAMINO.

EGIS forwards the vetting information electronically to CBP ATS. ATS acts strictly as a conduit, which will pass the information through to NCTC and does not store any information. NCTC reviews the information and sends back results, which once again will be passed through ATS strictly as a conduit to CAMINO. USCIS uses this information to assist in identifying

[35] *See* WRAPS PIA and SORN, *available at* https://2001-2009.state.gov/documents/organization/101146.pdf.
[36] *See* DHS/USCIS/PIA-051 Case and Activity Management for International Operations (CAMINO), *available at* www.dhs.gov/privacy.
[37] *See* DHS/CBP/PIA-006(e) Automated Targeting System, *available at* www.dhs.gov/privacy.

terrorism-related grounds of inadmissibility. The "clear" or "not clear" results of the NCTC check are uploaded into CAMINO.

Category of Individuals Affected:

Individuals seeking refugee classification and resettlement in the United States are required to complete Form I-590, *Registration for Classification as Refugee* and the information is entered into WRAPS. Form I-590 collects information about the applicants, as well as about family members and other associates.[38]

Information Sharing:

RASS retrieves information from DOS WRAPS for ingestion into CAMINO. USCIS RASS also passes the DOS WRAPS information to CBP ATS.

Applicable System of Records Notice:

The following SORNs cover the collection, maintenance, and use of the information for refugee resettlement:

- Refugee Case Processing and Security Screening Information SORN covers the collection, use, maintenance, and dissemination of refugee data, to include application intake, security checks, and adjudication;[39]
- DOS Refugee Case Records SORN covers the collection of information from individuals who have applied for admission to the United States as refugees that is stored in WRAPS;[40] and
- Immigration Biometric and Background Check (IBBC) System of Records, which covers the collection, use, and storage of biometric and biographic data for background checks and its results, covers background checks and their results.[41]

Retention:

USCIS EGIS RASS temporarily retains the limited biographic information. This temporary retention period is generally less than 30 minutes and no longer than 12 hours. Information is not transmitted to other parts of DHS.

---

[38] Associates are voluntarily provided by the applicant as part of the family tree and could include points of contact in the United States and other individuals with whom the applicant associates. Part of the reason these points of contact are provided are for determining the applicant's geographic location of resettlement in the United States.
[39] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (Oct. 19, 2016).
[40] *See* STATE-59 Refugee Case Records, 77 FR 5865 (Feb. 6, 2012).
[41] *See* DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), 83 FR 36950 (July 31, 2018).

APPENDIX D

USCIS Visa Support Services (VSS)

Background:

The Visa Support Services (VSS) allows for USCIS ASCs to collect biometric and limited biographic information from individuals physically present in the United States who are seeking immigration benefits from a partner country. This prevents the applicant from having to travel to the participating country to provide information. Upon collection, USCIS temporarily retains the biometric and biographic information captured pending notice of successful transmission to the partner country. USCIS then deletes both the biographic and biometric information after the partner country confirms receipt of it. The data collected at the ASCs is not used by USCIS for any purpose. USCIS provides this service to certain partner countries for a fee agreed upon by each country and set forth in a Memorandum of Understanding (MOU).[42]

Information Collected, Retained, and Disseminated and Source(s) of any PII and SPII:

Applicants submit their biographic information via their visa application. USCIS ASC personnel collect the biometric data. Through this project, the following categories of information are collected: full name, date of birth, country of birth, sex, nationality, fingerprints, and a photograph.

Category of Individuals Affected:

Individuals seeking immigration benefits with the partner country.

Information Sharing:

USCIS collects biographic and biometrics from individuals who are seeking immigration benefits from partner countries.

Applicable System of Records Notice:

USCIS temporarily retains information collected on behalf of a partner country for only as long as it takes to successfully transmit the information to the partner country. While temporarily retained, USCIS does not retrieve the records using a unique personal identifier. USCIS transfers the biographic information and biometric capture to the partner country immediately after collection. USCIS deletes the information from EGIS after the partner country provides confirmation of the successful transfer of the information. Therefore, no SORN is required to cover this collection.

Retention:

[42] Several countries have partnered with DHS USCIS to collect the requisite biometrics and limited biographical information on behalf of their immigration services.

VSS temporarily retains the limited biographic and biometric information. This temporary retention period is generally less than 30 minutes and no longer than 12 hours. Information is not transmitted to other parts of DHS.