



Privacy Impact Assessment

for the

Enterprise Gateway and Integration Services (EGIS)

DHS Reference No. DHS/USCIS/PIA-080(a)

March 18, 2022



Homeland
Security



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. The Enterprise Gateway and Integration Services acts as a conduit for the exchange of information between systems within USCIS, the U.S. Department of Homeland Security (DHS), external government agencies, and authorized third parties. USCIS is updating this Privacy Impact Assessment (PIA) to (1) account for 15 Enterprise Gateway and Integration Services system functionalities being deployed to support modernization of USCIS internal processes and workflows, and (2) expand the documented internal and external information sharing activities as all current information sharing activities supported by the Enterprise Service Bus 2 (ESB 2) which will continue to be supported by Enterprise Gateway and Integration Services as the Enterprise Service Bus 2 applications and services are transitioned. While all new functionalities have been documented in this Privacy Impact Assessment update, not all the system changes involve the collection, use, storage, or transmission of personally identifiable information.

Overview

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 Enterprise Service Bus 2 to the Enterprise Gateway and Integration Services to connect and share data from different operating USCIS systems.²

As stated in the previous Privacy Impact Assessment,³ the Enterprise Gateway and Integration Services 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, the Enterprise Gateway and Integration Services formats the message from one system to a different format to enable effective and secure synchronization and integration of data. To achieve system interoperability, both

¹ See “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017, *available at* <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE SERVICE BUS 2 (ESB 2), DHS/USCIS/PIA-008 (2007 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

³ The original EGIS PIA provides a list of services for which USCIS EGIS facilitates data synchronization and integration. See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE GATEWAY AND INTEGRATION SERVICES (EGIS), DHS/USCIS/PIA-080 (2019), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



systems must refer to a common information exchange reference model. As a backend system, the Enterprise Gateway and Integration Services reconciles different operating systems and standards in order to address interoperability complexities and challenges. The Enterprise Gateway and Integration Services does not retain any operational information.

Reason for the PIA Update

USCIS has begun to implement the second iteration of the Enterprise Gateway and Integration Services which supports the inclusion of additional system functionality to be implemented during the 2020 and 2021 calendar years. Most, but not all, of these new system functionalities involve the collection, use, transmission, or storage of personally identifiable information. Furthermore, many of these services were previously supported by legacy Enterprise Service Bus 2, but have transitioned into the Enterprise Gateway and Integration Services. System functionalities that do not involve personally identifiable information have been included within this Privacy Impact Assessment for transparency purposes and to provide a wholistic view of the Enterprise Gateway and Integration Services.

USCIS intends to implement the following functionalities:

Enterprise-wide services provided by Enterprise Gateway and Integration Services

- **Enterprise Gateway and Integration Services-Reference Data as a Service (RefDaaS):** This service within Enterprise Gateway and Integration Services is used to consistently provide standardized numbering and index data typically resident in existing Enterprise Service Bus 2 functions (e.g., United States Postal Service (USPS) Zip Codes, USCIS Country Codes).
- **Enterprise Gateway and Integration Services-Common Services (EGIS-CS):** This service within the Enterprise Gateway and Integration Services will provide general enterprise-wide capabilities in support of USCIS systems. The Enterprise Gateway and Integration Services-Common Services will enable USCIS to build enterprise services that can be used by multiple systems or applications rather than employ a traditional system development style where unique versions of the same service must be built for every different application or system. Enterprise Gateway and Integration Services 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 service access and interface access. Enterprise Gateway and Integration Services-Common Services includes functionality previously found in Enterprise Service Bus 2 (e.g., error handling services, logging services) and additional functionality (e.g., authentication services, encryption services) that are common to most services included in the Enterprise Gateway and Integration Services system. Enterprise Gateway and Integration Services-



Common Services also employs auditing measures to prevent inappropriate dissemination of data and to facilitate incident forensics, which is the collection and examination of digital evidence residing on electronic systems and the subsequent response to threats and attacks.

- **Enterprise Gateway and Integration Services-Snapshot Service:** This service within EGIS receives form data from the tasking USCIS systems and accurately produces specified forms as either Hypertext Markup Language (HTML) or Portable Document Format (PDF) files returned to the tasking USCIS system.
- **Enterprise Gateway and Integration Services-Payments Service:** This service within EGIS provides a payment transaction interface to the Treasury Department's Pay.Gov⁴ for all eProcessing⁵ Forms. Once Pay.Gov validates the payment information, the account holder is routed back to USCIS. A record of all transactions is saved in Amazon Web Services (AWS) database.
- **Third Party Integration (3PI):** This service within Enterprise Gateway and Integration Services will act as the single electronic gateway for third party software providers to do business with USCIS. Third Party Integration will serve as a conduit for intake of validated applicant data, which will be stored in USCIS case management systems. The details of which system processes a filing type will not be visible to third parties. This interface will operate in a one-way stream and only allow the ingestion of validated payloads. No other communication or information will be passed back to the client besides a transmission status message (transmission complete/incomplete).

System-specific services provided by Enterprise Gateway and Integration Services

- **Enterprise Gateway and Integration Services-Validation Instrument for Business Enterprises (EGIS-VIBE):** This service within Enterprise Gateway and Integration Services assists the Validation Instrument for Business Enterprises⁶ system with validating the business operations of companies and organizations seeking to employ foreign workers

⁴ See U.S. DEPARTMENT OF TREASURY, BUREAU OF THE FISCAL SERVICE, PRIVACY AND CIVIL LIBERTIES IMPACT ASSESSMENT FOR THE PAY.GOV, (2020), available at <https://www.fiscal.treasury.gov/files/pia/paygov-pclia.pdf>.

⁵ USCIS launched the eProcessing initiative to eliminate the creation of new paper immigration records. USCIS is moving from a traditional paper-based environment to a digital environment in which the immigration related request filing, adjudication, and communication are all electronic. As USCIS moves towards a digital environment, USCIS is fundamentally shifting its immigration records management processes and technologies. USCIS has historically used large systems with siloed operational functions to perform its case management needs. As part of the eProcessing initiative, USCIS plans to leverage and integrate existing operational systems with new services in an effort to enhance the processing of electronically filed immigration related request forms. Immigration files currently in paper form will remain as such until an individual affirmatively requests an additional benefit or until the record is otherwise used in an administrative context.

⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE VALIDATION INSTRUMENT FOR BUSINESS ENTERPRISES (VIBE), DHS/USCIS/PIA-044 (2014 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



in the United States. USCIS uses commercial information to verify a petitioning⁷ entity's qualifications for the benefit requested, to assess a petitioning entity's financial viability for cases that require the petitioning entity to establish ability to pay, and to provide a basis for a score that assists Immigration Services Officers (ISO) in identifying possible fraud concerns or contradictory information submitted by the petitioning entity. Enterprise Gateway and Integration Services-Validation Instrument for Business Enterprises enables the independent verification of petitioner information for immigrant and non-immigrant employment-based visas. Enterprise Gateway and Integration Services-Validation Instrument for Business Enterprises verifies the actual financial viability of the petitioning organization using open source data from an independent data service provider (e.g., Dun and Bradstreet (D&B)) to validate and verify the information provided by petitioning organizations. Enterprise Gateway and Integration Services-Validation Instrument for Business Enterprises communicates with Enterprise Gateway and Integration Services-Common Services, Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR),⁸ CLAIMS 3,⁹ Verification Information System (VIS),¹⁰ and Dun and Bradstreet systems.¹¹ Note: this Enterprise Gateway and Integration Services was previously provided by the Enterprise Service Bus 2.

- **Enterprise Gateway and Integration Services-Business Enterprise Query System (BEQS) (EGIS-BEQS):** The Enterprise Gateway and Integration Services will be used to send a company name and address to Dun and Bradstreet, whereby Dun and Bradstreet can

⁷ A petitioner is defined as a U.S. citizen or lawful permanent resident family member or employer (or the employer's agent) who files a family-based or employment-based immigrant visa petition with USCIS.

⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENTS FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>. See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM, DHS/USCIS/PIA-006 (2011 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹¹ Dun & Bradstreet, Inc. provides commercial data, analytics, and insights for businesses. Dun and Bradstreet collects information directly from businesses and business professionals when they participate in online services, such as apply for a Dun and Bradstreet D-U-N-S® Number. Dun and Bradstreet also collects information offline from business owners and principals, from businesses' creditors, vendors and suppliers, and from public records such as business registrations and bankruptcy filings. Dun and Bradstreet provides businesses and business professionals with access to their information within the Dun and Bradstreet databases and with an opportunity to correct verified inaccuracies. See DUN & BRADSTREET, *available at* <https://www.dnb.com/>.



match the information provided with its records, and then return additional information about the company to USCIS. The Verification Information System, which supports the E-Verify and Systematic Alien Verification for Entitlements (SAVE)¹² Programs, will use this interface in real-time; the Validation Instrument for Business Enterprises adjudication algorithm also uses data provided by Enterprise Gateway and Integration Services-Business Enterprise Query System.

- **Enterprise Gateway and Integration Services-Enterprise Document Management Service (EDMS)¹³ Support Services (EGIS-ESS):** The Enterprise Gateway and Integration Services supports the transfer of Immigrant Visa (IV) notifications, supporting documentation, and recorded data between USCIS and the U.S. Department of State (DoS). Enterprise Gateway and Integration Services-Enterprise Document Management Service Support Services facilitates communication between USCIS's Central Index System 2 (CIS 2),¹⁴ U.S. Immigration and Customs Enforcement's (ICE) Office of the Principal Legal Advisor (OPLA) Case Management System (OCMS),¹⁵ and USCIS's FOIA Immigration Records System (FIRST)¹⁶ with the Enterprise Document Management System. Note: this Enterprise Gateway and Integration Services functionality was previously provided by the Enterprise Service Bus 2 but was removed from Enterprise Service Bus 2 in 2018. Enterprise Gateway and Integration Services-Enterprise Document Management Service Support Services also includes some external partner connections previously provided by Enterprise Service Bus 2-Transformation Support Service (ESB-TSS).
- **Enterprise Gateway and Integration Services-Verification Service (EGIS-VS):** This functionality within Enterprise Gateway and Integration Services supports the Employee Eligibility Verification (EEV) program and allows authorized USCIS personnel the ability to search for information against multiple sources via one operation to verify claimed information. E-Verify¹⁷ leverages the Enterprise Gateway and Integration Services-

¹² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM, DHS/USCIS/PIA-006 (2011 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED DIGITIZATION DOCUMENT MANAGEMENT PROGRAM (IDDMP), DHS/USCIS/PIA-003 (2007 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 (2009 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF THE PRINCIPAL LEGAL ADVISOR (OPLA) CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-036 (2013 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-ice>.

¹⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FOIA IMMIGRATION RECORDS SYSTEM (FIRST), DHS/USCIS/PIA-077 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY



Verification Service as its automated primary verification process for employee verification. The Enterprise Gateway and Integration Services-Verification Service extracts verification information from USCIS CLAIMS 4,¹⁸ ICE's Student and Exchange Visitor Information System (SEVIS),¹⁹ and U.S. Customs and Border Protection's (CBP) TECS,²⁰ and the National Law Enforcement Telecommunications System (NLETS) via the EGIS-National Law Enforcement Telecom Service subsystem. Note: this Enterprise Gateway and Integration Services functionality was previously provided by the Enterprise Service Bus 2.

- **Enterprise Gateway and Integration Services-Person Centric Query Service (PCQS):**²¹ This functionality within the Enterprise Gateway and Integration Services allows a system or a person to submit a single query using an individual's A-Number for all transactions involving an immigrant across various USCIS and DoS systems. In response to the single query, the user would receive a consolidated and correlated view of the immigrants' past interactions with the government as he or she passed through the U.S. immigration system. Person Centric Query Service allows authorized users to submit a single query and view all permissible transactions users have been authorized to view, involving an immigrant or nonimmigrant across multiple DHS and external systems. The Employee Eligibility Verification program uses the Enterprise Gateway and Integration Services-Person Centric Query Service as its secondary verification process to complement the Enterprise Gateway and Integration Services-Verification Service. Enterprise Gateway and Integration Services-Person Centric Query Service auxiliary services also include Enterprise Gateway and Integration Services-EOIR-Court Schedule, which queries case scheduling information from the Executive Office for Immigration Review (EOIR)'s Case Access System (CASE),²² for staff information and availability, and USCIS's internal

IMPACT ASSESSMENT FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 4), DHS/USCIS/PIA-015 (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001 (2020 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-ice>.

²⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS), DHS/CBP/PIA-009 (2010 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

²¹ U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

²² The Case Access System (CASE) is the Information Resource Management System that provides the Executive Office for Immigration Review (EOIR) with case tracking and management information, office automation, Internet/Intranet, and automated legal research services. More information is available at



COVID contact tracking microservices. Note: this Enterprise Gateway and Integration Services was previously provided by the Enterprise Service Bus 2.

- **Enterprise Gateway and Integration Services-Customer Profile Management System (CPMS)-Support Services (EGIS-CPMS-SS):** This functionality within Enterprise Gateway and Integration Services facilitates communication between Application Support Center (ASC) Biometric Capture stations, the Office of Biometric Identity Management's (OBIM) Homeland Advanced Recognition Technology (HART),²³ the Federal Bureau of Investigation's (FBI) National Name Check Program,²⁴ and the Department of Defense's (DoD) Automated Biometric Identification System (ABIS)²⁵ with USCIS's Customer Profile Management System (CPMS).²⁶ Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services also facilitates the exchange of document information required by all case management systems in USCIS to produce benefit documents as well as notices sent to applicants. Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services also facilitates the exchange of biometric and biographic information collected from the Office of the United Nations High Commissioner for Refugees (UNHCR)²⁷ to the Office of Biometric Identity Management's Homeland Advanced Recognition Technology. Note: this EGIS service was previously provided by the Enterprise Service Bus 2.
- **Enterprise Gateway and Integration Services-American Association of Motor Vehicle Administrators (AAMVA) Hub Services (AHS) (EGIS-AHS):** This function within Enterprise Gateway and Integration Services is a collection of interfaces and business logic that facilitate the transmission of information between American Association of Motor Vehicle Administrators and multiple USCIS subsystems. Note: this EGIS service was previously provided by the ESB 2.
- **Enterprise Gateway and Integration Services-Security Center Operations (SCOPS) Intake Service (EGIS-SCOPS):** This function within Enterprise Gateway and Integration

<https://www.justice.gov/eoir/major-information-systems>.

²³ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

²⁴ The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI). See DOJ/FBI-002 Central Records System (CRS), 66 Fed. Reg. 29994 (June 4, 2001).

²⁵ See Department of Defense Detainee Biometric Information System, 72 Fed. Reg. 14534 (March 28, 2007).

²⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

²⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES (UNHCR) INFORMATION DATA SHARE, DHS/USCIS/PIA-081 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



Services enables the electronic connection and messaging from USCIS Security Center Operations Applicant Service Centers (ASC) providers (i.e., California, Nebraska, Texas, and Vermont Service Centers) to the backend USCIS IT systems. These backend systems currently consist of the Electronic Document Management System (EDMS), which is the USCS system of records, that stores the scanned PDF case image files (i.e., I-129 forms submitted from the Applicant Service Centers), and the DoS Kentucky Consular Center (DoS KCC), which is used for adjudicating the Non-Immigrant workers' Visa entries to the United States. Enterprise Gateway and Integration Services-Security Center Operations performs all legacy operational business functions and augments the case files received as a part of the adjudication process. This service also provides secure file messaging services between USCIS and DoS systems. Note: this function in Enterprise Gateway and Integration Services was previously provided by the Enterprise Service Bus 2.

- **Enterprise Gateway and Integration Services-National Law Enforcement Telecom Service (NLETS) (EGIS-NLETS):** Enterprise Gateway and Integration Services verifies information related to individual's driver's licenses, driver's permits, and state-issued ID cards. Once a request is sent by USCIS, it is received by National Law Enforcement Telecom Service and then sent to the U.S. Department of Justice (DOJ) National Law Enforcement Telecom Service system. EGIS-National Law Enforcement Telecom Service will then receive a response and relay the National Law Enforcement Telecom Service response to the tasking system. Note: this function in the Enterprise Gateway and Integration Services was previously provided by the Enterprise Service Bus 2.

This Privacy Impact Assessment update also expands internal and external information beyond sharing as outlined in the original Enterprise Gateway and Integration Services Privacy Impact Assessment published in June 2019. USCIS currently shares information from USCIS with other federal agencies for the purpose of processing applications, requests, or petitions under the Immigration and Nationality Act via Enterprise Service Bus 2. The Enterprise Service Bus 2 may also share information 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 System of Records Notice (SORN). The Enterprise Service Bus 2 services may share electronic USCIS information with outside entities, either pursuant to regulation or through specific agreements. These information sharing activities were previously documented in the published the Enterprise Service Bus 2 Privacy Impact Assessments.²⁸ The systems transitioning from being supported by Enterprise Service Bus 2 to being supported by the Enterprise Gateway and Integration Services will continue to share information in accordance with

²⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE SERVICE BUS 2 (ESB 2), DHS/USCIS/PIA-008(a) (2007 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



the established information sharing agreements. The transition to Enterprise Gateway and Integration Services from Enterprise Service Bus 2 will not change or expand the established information sharing activities. This continued sharing is described above within the outline of the Enterprise Gateway and Integration Services and is further detailed within this Privacy Impact Assessment

Privacy Impact Analysis

Authorities and Other Requirements

As stated in the previous Privacy Impact Assessment, USCIS collects and uses information under the authority of the Immigration and Nationality Act.²⁹ Specifically, 8 U.S.C. § 1103 charges the Secretary of Homeland Security with the duty of administering and enforcing laws relating to the immigration and naturalization of undocumented individuals.

The Enterprise Gateway and Integration Services Authority to Operate (ATO) is pending adjudication and publication of this Privacy Impact Assessment. The Enterprise Gateway and Integration Services plans to transition into the Ongoing Authorization (OA) program upon completion of this Privacy Impact Assessment and finalization of the Authority to Operate. Ongoing Authorization requires Enterprise Gateway and Integration Services to be reviewed by USCIS Ongoing Authorization Team on a monthly basis and maintain its security and privacy posture to maintain its Authority to Operate.

Characterization of the Information

With this update, there are no changes to the Characterization of the Information detailed in the published June 2019 Enterprise Gateway and Integration Services Privacy Impact Assessment. Enterprise Gateway and Integration Services continues to be an intermediary system, meaning that it connects different source systems together to enable communication among them. The Enterprise Gateway and Integration Services continues to depend on the accuracy and quality of information from each source system and ensures the accuracy of the data by collecting the information directly from the source systems. There are no additional risks to the Characterization of the Information.

Uses of the Information

With this update, there are no changes to the Uses of the Information detailed in the published June 2019 Enterprise Gateway and Integration Services Privacy Impact Assessment. The purpose of the Enterprise Gateway and Integration Services continues to support the integration of legacy and different operating systems by enabling the seamless integration,

²⁹ See 8 U.S.C. § 1101 et seq.



communication, and exchange of data between systems. There are no additional risks to the Uses of the Information.

Notice

With this update, there are no changes to how notice is provided to individuals detailed in the published June 2019 Enterprise Gateway and Integration Services Privacy Impact Assessment. The Enterprise Gateway and Integration Services does not collect information directly from individuals. USCIS provides general notice to individuals seeking USCIS benefits through a Privacy Notice contained on all USCIS forms/instructions. There are no additional risks to Notice.

Data Retention by the Project

With this update, there are no changes to the Data Retention detailed in the published June 2019 Enterprise Gateway and Integration Services Privacy Impact Assessment. The Enterprise Gateway and Integration Services continues to not save data from any of the systems that are connecting through the Enterprise Gateway and Integration Services and does not maintain/retain any data once the data is exchanged. There are no additional risks to Data Retention.

Information Sharing

This update expands internal and external information beyond sharing as outlined in the Enterprise Gateway and Integration Services Privacy Impact Assessment published in June 2019.

USCIS currently shares information from USCIS with other federal agencies for the purpose of processing applications, requests, or petitions under the Immigration and Nationality Act via Enterprise Service Bus 2. Enterprise Service Bus 2 may also share information 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 System of Records Notice. The Enterprise Service Bus 2 services may share electronic USCIS information with outside entities, either pursuant to regulation or through specific agreements. These information sharing activities were previously documented in the published Enterprise Service Bus 2 Privacy Impact Assessments.³⁰

The systems transitioning from being supported by Enterprise Service Bus 2 to being supported by Enterprise Gateway and Integration Services will continue to share information in accordance with the established information sharing agreements. The transition to Enterprise Gateway and Integration Services from Enterprise Service Bus 2 will not change or expand the established information sharing activities. The following information sharing activities will

³⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE SERVICE BUS 2 (ESB 2), DHS/USCIS/PIA-008 (2007 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



transition from being supported by Enterprise Service Bus 2 to being supported by system specific services provided by Enterprise Gateway and Integration Services:

Department of Defense (DoD)

Through the Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services, USCIS sends both biographic and biometric information to DoD to conduct checks on individuals, as well as their eligible family members, seeking refugee or asylum protections. All DoD check requests, responses, and queries flow through EGIS-Customer Profile Management System-Support Services, which connects DoD Automated Biometric Identification System and Customer Profile Management System.

USCIS, via Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services, sends the benefit requestor's date of birth, country of birth, race, ethnicity, weight, height, eye color, hair color, gender, address, and biometric images (i.e., fingerprints, photograph, and signature) to DoD in order to conduct the background check. The DoD check is an image-based search of the DoD's Automated Biometric Identification System.³¹ Automated Biometric Identification System contains DoD encounter history information compiled during its operations and from individuals seeking access to its installations. USCIS only sends fingerprints to Automated Biometric Identification System for specific benefit types when the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military. Currently, those specific benefit types are refugee, asylum, and international relative petitions related to those benefit types.³² DoD responds to the check with either "Non-Match" or "Match." A Non-Match response means that DoD has no encounter history information related to the fingerprints submitted by the benefit requestor. A Match response means DoD had obtained fingerprints from the same individual who had submitted fingerprints to USCIS. Match responses are accompanied by pertinent text explaining the nature of the previous DoD encounter.

Sharing USCIS data with DoD is compatible with the purpose for which it was initially collected because USCIS is required to conduct background and security checks to identify threats to national security and public safety posed by those seeking immigration benefits. The external sharing of biographic information with DoD is covered under routine use Q of DHS/USCIS-018 Immigration Biometric and Background Check System of Records Notice,³³ which allows USCIS to disclose information with DoD to verify an applicant's eligibility for the requested benefit.

³¹ See Department of Defense Detainee Biometric Information System, 72 Fed. Reg. 14534 (March 28, 2007).

³² DoD retention of these biometrics varies based on benefit type.

³³ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.



Department of Justice (DOJ), Federal Bureau of Investigation (FBI)

USCIS sends immigration requestor information to the FBI to conduct name checks through Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services. All FBI Name Check requests, responses, and queries flow through the EGIS-Customer Profile Management System-Support Services; there is no direct connection between the FBI systems and Customer Profile Management System.

The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI).³⁴ Central Records System contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement and national security purposes. Universal Index consists of administrative, benefit requestor, criminal, personnel, and other law enforcement files. The FBI responds to the FBI Name Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information based on the name and DOB of the benefit requestor. A pending response means further research is needed before the FBI can provide a definitive response. For those records with an initial response of pending, the FBI will complete a review of its records and provide a final response of no record or positive response. A positive response means the FBI has information relating to the subject, which is then obtained by USCIS officers through separate processes outside of Customer Profile Management System.

USCIS simultaneously sends benefit requestor information, to include, name, DOB, country of birth, race, gender, address, and biometric images (including photographs and fingerprints) to both the Automated Biometric Identification System/Homeland Advanced Recognition Technology and FBI Next Generation Identification (NGI) in order to conduct the background check.³⁵ Next Generation Identification contains FBI criminal history record information compiled from law enforcement and national security submitters. The FBI check is an image-based search of Next Generation Identification. The FBI responds to the check with either a: "Non-Match," "Match," or unclassifiable. A Non-Match response means that the FBI has no criminal history information related to the fingerprints captured from the benefit requestor. A Match response means the FBI has criminal history information relating to the fingerprints submitted. A Match response is usually accompanied by the Identity History Summary, previously known as the Record of Arrest and Prosecution Sheet (RAP Sheet). An unclassifiable response means the fingerprint image quality was too poor to compare against fingerprint records contained within the Automated Biometric Identification System/Homeland Advanced Recognition

³⁴ See DOJ/FBI-002 Central Records System (CRS), 66 Fed. Reg. 29994 (June 4, 2001).

³⁵ The FBI replaced its Integrated Automated Fingerprint Identification System (IAFIS) with the Next Generation Identification (NGI). Please see the Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, *available at* <https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngiinteroperability-1>.



Technology and Next Generation Identification. For those records with an initial response of unclassifiable, USCIS captures and submits additional fingerprints to obtain a valid response.

Sharing USCIS data with the FBI is compatible with the purpose for which it was initially collected because USCIS is required to conduct background and security checks to identify grounds of ineligibility for the requested benefit, to include threats to national security and public safety posed by those seeking immigration benefits. The external sharing of biographic and biometric information with the FBI is covered under Routine Use O of the DHS/USCIS-018 Immigration Biometric and Background Check System of Records Notice,³⁶ which allows USCIS to share information in Customer Profile Management System with the FBI to verify the applicant's eligibility for the benefit being sought.

Department of Justice (DOJ), Executive Office for Immigration Review (EOIR)

USCIS Enterprise Gateway and Integration Services-Person Centric Query Service auxiliary service, Enterprise Gateway and Integration Services-Executive Office for Immigration Review-Court Schedule, queries case scheduling information from the Executive Office for Immigration Review's Case Access System (CASE)³⁷ for staff information and availability. Enterprise Gateway and Integration Services-Person Centric Query Service does not send information to Executive Office for Immigration Review.

Department of State (DoS)

Enterprise Gateway and Integration Services continues to share data with DoS in accordance with the sharing outlined in the published June 2019 Enterprise Gateway and Integration Services Privacy Impact Assessment. Enterprise Gateway and Integration Services shares information from USCIS to DOS for the purpose of processing applications and petitions under the Immigration and Naturalization Act. The Enterprise Gateway and Integration Services-Adoption Case Management System (ACMS) Orchestration Services (EGIS-ACMS-AOS) and the Enterprise Gateway and Integration Services-Refugee Asylum Support Service (RASS) (EGIS-RASS) services facilitate the sharing of benefit requestor information with DoS.

Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services continues to facilitate the secure connection between the USCIS Adoption

³⁶ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.

³⁷ The Case Access System (CASE) is the Information Resource Management System that provides the Executive Office for Immigration Review (EOIR) with case tracking and management information, office automation, Internet/Intranet, and automated legal research services. More information is available at <https://www.justice.gov/eoir/major-information-systems>.



Case Management System (ACMS)³⁸ and the DoS Consolidated Consular Database (CCD)³⁹ in support of inter-country adoptions. USCIS adjudicators are able to electronically share intercountry adoption filings from Adoption Case Management System to DoS' Consolidated Consular Database through Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services. Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services reads the message from Adoption Case Management System, transforms the data using the mappings defined in the EGIS service, and updates DoS' Consolidated Consular Database in a compatible format. Adoption Case Management System transmits an encrypted adoption message to Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services using the USCIS Data Streaming Services.⁴⁰ Using the Data Streaming Service, Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services can securely decrypt, validate, and transform the adoption application from Adoption Case Management System into the required message format for delivery to DOS. Once processed by Enterprise Gateway and Integration Services-Adoption Case Management System Orchestration Services, the application information is once again encrypted and sent to the DoS' Consolidated Consular Database using the Consolidated Consular Database web service.

Enterprise Gateway and Integration Services-Refugee Asylum Support Service retrieves refugee case information from DoS Worldwide Refugee Admissions Processing System (WRAPS)⁴¹ for ingestion into the Case and Activity Management for International Operations (CAMINO).⁴² EGIS-Refugee Asylum Support Service also passes the DOS Worldwide Refugee Admissions Processing System information to CBP's Automated Targeting System (ATS).⁴³ CBP's Automated Targeting System acts strictly as a conduit, which will pass the information through to National Counter Terrorism Center (NCTC) and does not store any information. The

³⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE DOMESTICALLY FILLED INTER-COUNTRY ADOPTION APPLICATIONS AND PETITIONS, DHS/USCIS/PIA-007 (2016 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

³⁹ See U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE DOS CONSULAR CONSOLIDATED DATABASE (CCD), available at <https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf>.

⁴⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE DATA STREAMING SERVICES, DHS/USCIS/PIA-078 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁴¹ See U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT AND SYSTEM OF RECORDS NOTICE FOR THE WRAPS, available at <https://www.state.gov/wp-content/uploads/2020/06/Worldwide-Refugee-Admissions-Processing-System-WRAPS-PIA.pdf>.

⁴² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CASE AND ACTIVITY MANAGEMENT FOR INTERNATIONAL OPERATIONS (CAMINO), DHS/USCIS/PIA-051 (2020 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁴³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



National Counter Terrorism Center reviews the information and sends back results, which once again will be passed through CBP's Automated Targeting System strictly as a conduit to the Case and Activity Management for International Operations system via EGIS-Refugee Asylum Support Service. USCIS uses this information to assist in identifying terrorism-related grounds of inadmissibility. The "clear" or "not clear" results of the National Counter Terrorism Center check are uploaded into the Case and Activity Management for International Operations system, which is then used by USCIS personnel to compile and provide a final response to DoS Worldwide Refugee Admissions Processing System. 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. This sharing enables vetting of DoS Worldwide Refugee Admissions Processing System data against each agency's respective holdings to identify possible derogatory information related to individuals seeking refugee status.

With this update, Enterprise Gateway and Integration Services will begin to support existing USCIS-DoS sharing previously supported by Enterprise Service Bus 2. Enterprise Gateway and Integration Services-Person Centric Query Service and Enterprise Gateway and Integration Services-Enterprise Document Management Service Support Services facilitate the sharing of immigration requestor information with DoS. Enterprise Gateway and Integration Services-Person Centric Query Service provides authorized DoS users direct access to USCIS systems. Sharing USCIS data with DoS is compatible for which it was initially collected because the DoS mission, like USCIS, includes processing immigration requests under the Immigration and Nationality Act to ensure visits and immigration to the United States are lawful.

USCIS shares information with DoS as permitted under the following routine uses:

- Routine Use O of DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records Notice⁴⁴ permits the disclosure of information with the DoS in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements; or when the DoS requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an undocumented individual or an enforcement operation with transnational implications.
- Routine Use I of the DHS/USCIS-007 Benefits Information System System of Records Notice⁴⁵ permits the disclosure of information with the DoS to assist with the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all

⁴⁴ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁴⁵ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.



other immigration and nationality laws and treaties and reciprocal agreements entered into in furtherance of the enforcement of U.S. immigration and nationality laws.

- Routine Use K of DHS/USCIS-010 Asylum Information and Pre-Screening System of Records Notice⁴⁶ permits the disclosure of information with the DoS for the purpose of assisting in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws and treaties and reciprocal agreements entered into in furtherance of the enforcement of U.S. immigration and nationality laws.
- Routine Use P of the DHS/USCIS-018 Immigration Biometric and Background Check System of Records Notice⁴⁷ permits the sharing of information with the DoS in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws and treaties and reciprocal agreements entered into in furtherance of the enforcement of U.S. immigration and nationality laws.

Department of the Treasury (Treasury)

After an individual has submitted the requisite fees through Pay.Gov, USCIS ELIS⁴⁸ receives payment confirmation through Enterprise Gateway and Integration Services-Enterprise Document Management Service Support Services from the Collection Information Repository (CIR). Sharing USCIS data with Treasury is compatible for which it was initially collected because Treasury collects and processes fee payments associated with immigration requests from individuals on behalf of USCIS. Routine Use Z of the DHS/USCIS-007 Benefits Information System of Records Notice⁴⁹ permits sharing information with Treasury to perform initial processing of immigration requests and to accept and resolve payment and any related issues.

U.S. Postal Service (USPS)

Address information provided by the benefit seeker is transmitted to USPS to obtain the USPS standardized address. No System of Records Notice is required for this external sharing because the data is not maintained in a system of records under the Privacy Act.

⁴⁶ See DHS/USCIS-010 Asylum Information and Pre-Screening, 80 Fed. Reg. 74781 (November 30, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁴⁷ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁴⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM, DHS/USCIS/PIA-056, (2018 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁴⁹ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.



American Association of Motor Vehicle Administrators (AAMVA)

Enterprise Gateway and Integration Services-American Association of Motor Vehicle Administrators Hub Services facilitates the secure connection between USCIS Verification Information System and American Association of Motor Vehicle Administrators in support of the Systematic Alien Verification for Entitlements. Disclosing USCIS data with American Association of Motor Vehicle Administrators is compatible with the purpose for which USCIS initially collected the information because the law permits employers to verify the information from a driver's license, permit, or state-issued ID card if the state has established a memorandum of agreement (MOA) with DHS USCIS to allow verification of this information. AAMVAnet is a conduit that provides access to biographical information collected by state Motor Vehicle Agencies (MVA). American Association of Motor Vehicle Administrators operates AAMVAnet; however, the data in the system is owned by the organization that had the original authority to collect the data.

National Law Enforcement Telecommunications System (NLETS)

In support of the E-Verify Program, USCIS established a secure connection between USCIS Verification Information System and National Law Enforcement Telecom Service to verify information related to individuals' driver's licenses, driver's permits, and state-issued ID cards. This sharing is supported by Enterprise Gateway and Integration Services-National Law Enforcement Telecom Service. Sharing USCIS data with National Law Enforcement Telecom Service is compatible with the purpose of the system because the law permits employers to verify the information from a driver's license, permit, or state-issued ID card if there is an information sharing agreement in place with DHS USCIS to allow verification of this information. National Law Enforcement Telecom Service is a conduit that provides access to biographical information collected by state Motor Vehicle Agencies (MVA). However, the data in the system is owned by the organization with the original authority to collect the data.

United Nations High Commissioner for Refugees (UNHCR)

On January 9, 2019, DHS entered into a Memorandum of Understanding (MOU) with United Nations High Commissioner for Refugees to share biometric and associated biographic data on refugees seeking to resettle in the United States. DHS and United Nations High Commissioner for Refugees entered into this Memorandum of Understanding to expand the scope of the existing information shared through the State Department to support the U.S. Refugee Admissions Program (USRAP). Under the 2019 Memorandum of Understanding, United Nations High Commissioner for Refugees directly shares biometric and associated biographic information with DHS Office of Biometric Identity Management's Automated Biometric Identification System



(IDENT)⁵⁰ (soon to be replaced by Homeland Advanced Recognition Technology⁵¹). The electronic transmission of data between United Nations High Commissioner for Refugees and Automated Biometric Identification System is facilitated by USCIS.

Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services facilitates the exchange of biometrics (e.g., fingerprints, photograph, and/or iris) along with basic biographic data (e.g., name, date of birth, place of birth, gender) collected from the Office of the United Nations High Commissioner for Refugees to OBIM's Automated Biometric Identification System. This information allows USCIS verify that the individual being processed by USCIS for refugee resettlement is the same individual who was registered and referred by United Nations High Commissioner for Refugees.⁵²

Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services is facilitating the exchange of information between United Nations High Commissioner for Refugees and OBIM's Automated Biometric Identification System (IDENT). United Nations High Commissioner for Refugees is sharing biometric and biographic information related to individuals seeking admission into the U.S. Refugee Admissions Program. The transfer of data is accomplished using the Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services. Upon receipt, Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services forwards the information to OBIM's Automated Biometric Identification System where it is retained. Enterprise Gateway and Integration Services-Customer Profile Management System-Support Services only facilitates the exchange of information from United Nations High Commissioner for Refugees and OBIM's Automated Biometric Identification System. USCIS does not retain or retrieve the records using a unique personal identifier. Therefore, System of Records Notice coverage is not required for this exchange of information.

The exchange of information from the United Nations High Commissioner for Refugees to OBIM is covered under the External Biometric Records System of Records Notice,⁵³ which discusses the use of biometric and associated biographic information from non-DHS entities, both

⁵⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

⁵¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

⁵² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES (UNHCR) INFORMATION DATA SHARE, DHS/USCIS/PIA-081 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁵³ See DHS/USCIS-041 External Biometric Records, 83 Fed. Reg. 17829 (April 24, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.



foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, and national defense.

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: This risk is mitigated. 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 System of Records Notices to verify the compatibility of an information exchange prior to disclosing data. DHS has Memoranda of Understanding/Agreement 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, Enterprise Gateway and Integration Services 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 Memoranda of Understanding/Agreement 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 the Enterprise Gateway and Integration Services may be inaccurate.

Mitigation: This risk cannot be fully mitigated. The Enterprise Gateway and Integration Services depends on the accuracy and quality of information from each source system. Enterprise Gateway and Integration Services ensures the accuracy of the data by collecting the information directly from the source systems. For data that may be transferred through the Enterprise Gateway and Integration Services, 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.



Redress

There are no changes in the risk associated with redress from the initial Privacy Impact Assessment. Enterprise Gateway and Integration Services does not store any records. Any redress mechanisms would come from the source system.

Auditing and Accountability

USCIS ensures that practices stated in this Privacy Impact Assessment comply with federal, DHS, and USCIS standards, policies, and procedures, including standard operating procedures, rules of behavior, and auditing and accountability procedures. The Enterprise Gateway and Integration Services is maintained in Amazon Web Services, 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. Amazon Web Services is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host personally identifiable information.⁵⁴

USCIS requires Enterprise Gateway and Integration Services 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 mitigate 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.

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 personally identifiable information. The privacy awareness training addresses appropriate privacy concerns, including Privacy Act obligations. The computer security awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information. USCIS also provides role-based training on the proper uses of USCIS information.

USCIS only grants back-end Enterprise Gateway and Integration Services access 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

⁵⁴ 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 is available at <https://www.fedramp.gov/>.



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.

Responsible Official

Angela Washington
Privacy Officer
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
(240) 721-3701

Approval Signature

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

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717



APPENDIX A: Adoption Orchestration Services (AOS)

No changes have been made to the AOS. Please refer to the July 2019 EGIS PIA.

APPENDIX B: Lockbox Intake Service (LIS)

No changes have been made to the LIS. Please refer to the July 2019 EGIS PIA.

APPENDIX C: EGIS Refugee Asylum Support Service (RASS)

No changes have been made to the RASS. Please refer to the July 2019 EGIS PIA.

APPENDIX D: USCIS Visa Support Services (VSS)

No changes have been made to the VSS. Please refer to the July 2019 EGIS PIA.



Appendix E

EGIS-Reference Data as a Service (EGIS-RefDaaS)

Background:

The EGIS-RefDaaS component serves to provide ordinal and index data typically resident in existing ESB 2 functions (e.g. United States Postal Service (USPS) zip codes and USCIS country codes). Reference data is best described by example, such as a list of approved and commonly shared data such as country code (2-character or 3 character), states, zip codes, hair colors, eye colors, races, ethnicities, and religion. These kinds of data are in fact updated at times (country names change for example) and new data sets are ingested over time on the behest of system owners that would like their referential data shared. These data elements have been combined in a service accessible by all other EGIS components. EGIS-RefDaaS is most typically used to populate user interfaces with drop down lists when users are filling out forms, having to select from the approved list of countries of birth, for example. The Office of the Chief Data Officer (OCDO) is an independent organization that presides over the standardization and correctness of the data. EGIS-RefDaaS simply warehouses the data for them and makes the data highly available. EGIS-RefDaaS is used by many other USCIS systems such as NASS, myUSCIS, and more.

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

This service does not collect, use, store, or transmit PII.

Category of Individuals Affected:

Reference Data is not related to specific individuals, but serves as a standardized repository for consistent data element enumeration.

Information Sharing:

Reference data in the form of ordinal data such as country codes and zip codes are shared between various USCIS systems.

Applicable System of Records Notice:

A System of Records Notice (SORN) is not required for EGIS-RefDaaS as it contains no PII or other sensitive information.

Retention:

Time contextualized reference data (including current and archival) is retained as directed by OCDO within limits of storage space and access time constraints.



Appendix F

EGIS-Common Services (EGIS-CS)

Background:

EGIS - Common Services (EGIS-CS) provides enterprise capabilities in support of Service Oriented Architecture, Business Process Management and Complex Event Processing. This service within EGIS will provide general enterprise-wide capabilities in support of USCIS systems. The EGIS-Common Services will enable USCIS to build enterprise services that can be used by multiple systems or applications rather than employ a traditional system development style where unique versions of the same service must be built for every different application or system.

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 service access and interface access. The EGIS-CS includes functionality found in ESB 2 (e.g., error handling services, logging services) and includes additional functionality (e.g., authentication services, encryption services) that are common to most services included in the EGIS system.

EGIS-CS 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. EGIS-CS also includes platform specific tools including portions of the EGIS system that allow for development and operation of the system, including configuration of the orchestration engine, messaging subsystems, and security tools that are specific to the EGIS system.

EGIS-CS includes Encryption as a Service (EaaS), which allows encryption of data at rest (e.g., data in temporarily placed in reusable Kafka queues). Iteration-2 will also include the Enterprise Audit Logging Service (EALS) to provide a centralized mechanism to capture application logs, event logs, audit logs and handle run-time exceptions, which are sent to Splunk to meet USCIS and DHS security requirements. and the iteration also includes the Email Service to provide common functionality for sending emails using USCIS SMTP service agent.

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

These tools themselves do not collect or store PII. This component may handle PII in encrypted transit. PII transiting the system using these tools will be addressed within the Appendices covering the specific components of EGIS (e.g., VSS, RASS).

Category of Individuals Affected:

Refer to the Appendices covering the specific components of EGIS (e.g., VSS, RASS) which uses the EGIS-CS.



Information Sharing:

Refer to the Appendices covering the specific components of EGIS (e.g., VSS, RASS) which uses the EGIS-CS.

Applicable System of Records Notice:

Refer to the Appendices covering the specific components of EGIS (e.g., VSS, RASS) which uses the EGIS-CS.

Retention:

Refer to the Appendices covering the specific components of EGIS (e.g., VSS, RASS) which uses the EGIS-CS.



Appendix G

EGIS-Snapshot Service

Background:

The EGIS Snapshot service provides RESTful endpoints that consume JavaScript Object Notation (JSON) form data and accurately produce corresponding forms in either HTML or PDF format. For example, an authorized program may send a JSON formatted message to the EGIS-Snapshot service that would complete USCIS Form I-539 *Application to Extend/Change Nonimmigrant Status*. The reply message would be the output byte stream for the PDF.

The EGIS-Snapshot service provides two primary features:

- Endpoints which consume JSON data and produce a document in either HTML or PDF format; and
- A utility endpoint to convert an HTML document to PDF (experimental).

Currently, this service is in production for the electronic submission of Form I-539 (since May 2019) and multiple forms are in the development process.

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

EGIS-Snapshot does not collect or store PII. This component may handle PII in encrypted transit. PII transiting the system using these tools will be addressed within the Appendices covering the specific components of EGIS (e.g., other Appendices within this PIA).

Category of Individuals Affected:

Individuals seeking to Extend/Change Nonimmigrant Status.

Information Sharing:

Refer to the Appendices covering the specific components of EGIS (e.g., other Appendices within this PIA) which uses the EGIS-Snapshot subsystem.

Applicable System of Records Notice:

Refer to the Appendices covering the specific components of EGIS (e.g., other Appendices within this PIA) which uses the EGIS-Snapshot subsystem.

Retention:

Refer to the Appendices covering the specific components of EGIS (e.g., other Appendices within this PIA) which uses the EGIS-Snapshot subsystem.



Appendix H

EGIS-Payment Service

Background:

The EGIS Payments service provides global payment services for all benefit types in support of the adjudication process. The EGIS Payments Service provides payment transaction interface to Pay.Gov (Treasury) for all eProcessing Forms. All transactions are saved in AWS PostgreSQL RDS database.

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

Payment reference number and status are consumed by the EGIS-Payments Service in order to verify completion of the payment no PII or Sensitive Financial Data is used within the EGIS-Payments Service subsystem

Category of Individuals Affected:

USCIS systems supporting individuals paying USCIS Fees electronically interface with the EGIS-Payments Service subsystem.

Information Sharing:

USCIS Transaction related payment information is shared with US Treasury and tasking USCIS systems. Applicants are directed into the U.S. Treasury payment portal www.pay.gov.

Applicable System of Records Notice:

USCIS does not collect or maintain financial or payment information involved during a transaction with Pay.gov. The Department of the Treasury, Bureau of the Fiscal Service FS 013 – Collections Records SORN⁵⁵ covers information collected and maintained about individuals who electronically authorize payments to the federal government, including through the use of Pay.gov.

Retention:

The EGIS Payments Service subsystem retains non-sensitive transaction related data (payment reference number and status) in a PostgreSQL database until no longer required by the tasking USCIS system.

⁵⁵ See Department of the Treasury, Bureau of the Fiscal Service FS 013 – Collections Records SORN, 85 Fed. Reg. 11776 (February 27, 2020), available at <https://home.treasury.gov/footer/privacy-act/system-of-records-notice-sorns>.



Appendix I

EGIS-Validation Instrument for Business Enterprises (EGIS-VIBE/VIBE+)

Background:

The EGIS Validation Instrument for Business Enterprises (EGIS-VIBE/VIBE+) service provides independent verification of petitioner information for employment-based visas. This service within EGIS assists the VIBE⁵⁶ system with validating the business operations of companies and organizations seeking to employ foreign workers in the United States. USCIS uses commercial information to verify a petitioning⁵⁷ entity's qualifications for the benefit requested, to assess a petitioning entity's financial viability for cases that require the petitioning entity to establish ability to pay, and to provide a basis for a score that assists Immigration Services Officers (ISOs) in identifying possible fraud concerns or contradictory information submitted by the petitioning entity. EGIS-VIBE enables the independent verification of petitioner information for immigrant and non-immigrant employment-based visas.

EGIS-VIBE verifies the actual financial viability of the petitioning organizations. It uses commercially available open-source data received via EGIS-BEQS from an independent data service provider, Dun and Bradstreet (D&B), to validate and verify the information provided by petitioning organizations. This information confirms petitioning organization validity and provides a baseline indicator of financial viability for that entity. To accomplish this, EGIS-VIBE communicates with EGIS-Common Services, Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR),⁵⁸ CLAIMS 3,⁵⁹ Verification Information System (VIS),⁶⁰ and D&B systems.⁶¹ The EGIS-VIBE user interface allows users to retrieve and

⁵⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE VALIDATION INSTRUMENT FOR BUSINESS ENTERPRISES (VIBE), DHS/USCIS/PIA-044 (2014 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁵⁷ A petitioner is defined as a U.S. citizen or lawful permanent resident family member or employer (or the employer's agent) who files a family-based or employment-based immigrant visa petition with USCIS.

⁵⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁵⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁶⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENTS FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>. See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM, DHS/USCIS/PIA-006 (2011 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁶¹ Dun & Bradstreet (D&B), Inc. Provides commercial data, analytics, and insights for businesses. D&B collects



consolidate data related to immigrant and non-immigrant employment-based petitions. This subsystem is the successor to the ESB2 subsystem entitled Validation Instrument for Business Enterprises (VIBE).

A parallel development effort is underway to enhance the front-end accessibility to EGIS-VIBE via a new interface (EGIS-VIBE+). EGIS-VIBE+ is currently being released in production to a subset of USCIS users. EGIS-VIBE+ will include all of the back-end functionality of legacy EGIS-VIBE as well as the new interface. Cutover to EGIS-VIBE+ is targeted for the near future with plans to sunset EGIS-VIBE shortly after.

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

EGIS-VIBE electronically receives company information from D&B via EGIS-BEQS and the petition information from CLAIMS 3 and VIBE.

Category of Individuals Affected:

USCIS uses EGIS-VIBE to assist in adjudicating employment-based immigration request forms and other benefits that are associated with a higher fraud risk.

Information Sharing:

VIBE uses EGIS-VIBE to interface with D&B, CLAIMS 3, and eCISCOR.

Applicable System of Records Notice:

The following SORNs cover the collection, maintenance, and use of EGIS-VIBE:

- Alien File, Index, and National File Tracking System,⁶² which covers the petition, supplemental evidence, and decision notices;
- Fraud Detection and National Security Records,⁶³ which covers the cases referred to CFDO for administrative inquiry and identified as benefit fraud; and
- Benefits Information System,⁶⁴ which covers the review of applications and petitions.

information directly from businesses and business professionals when they participate in online services, such as apply for a D&B DU-N-S@ Number. D&B also collects information offline from business owners and principals, from businesses' creditors, vendors and suppliers, and from public records such as business registrations and bankruptcy filings. D&B provides businesses and business professionals with access to their information within the D&B databases and with an opportunity to correct verified inaccuracies. See DUN & BRADSTREET, available at <https://www.dnb.com/>.

⁶² See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶³ See DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 Fed. Reg. 47411 (August 8, 2012), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁶⁴ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.



Retention:

The EGIS VIBE subsystem does not maintain/retain any data. The data is temporarily stored in a queue for few seconds for processing. Once successfully or unsuccessfully processed, the data is no longer available in the queue.



Appendix J

EGIS-Business Enterprise Query System (EGIS-BEQS)

Background:

The EGIS BEQS interface is used to send company name and address to Dun and Bradstreet (D&B), whereby D&B can match the information provided with its records, and then return additional information about the company to USCIS. It uses commercially available open-source data from an independent data service provider, Dun and Bradstreet (D&B), to validate and verify the information provided by petitioning organizations. This information confirms petitioning organization validity and provides a baseline indicator of financial viability for that entity. The Verification Information System (VIS) System uses this interface in real-time and VIBE adjudication algorithm uses data provided by EGIS-BEQS.

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

EGIS-BEQS electronically receives company only information from D&B and the petition information from VIBE.

Category of Individuals Affected:

USCIS uses EGIS-BEQS in conjunction with EGIS-VIBE to assist in adjudicating employment-based immigration request forms and other benefits that are associated with a higher fraud risk.

Information Sharing:

EGIS-BEQS interfaces with D&B, EGIS-VIBE, and VIBE

Applicable System of Records Notice:

EGIS-BEQS is does not retain records subject to a SORN.

Retention:

The EGIS-BEQS subsystem does not maintain/retain any data. The data is temporarily stored in a queue for few seconds for processing. Once successfully or unsuccessfully processed, the data is no longer available in the queue.



Appendix K

EGIS- Enterprise Document Management Service (EDMS) Support Services (EGIS-ESS)

Background:

The EGIS EDMS Support Service (EGIS-ESS), in its role as an Integration Service, supports the transfer of Immigrant Visa (IV) notifications and supporting documentation and recorded data between USCIS and DoS. EGIS-ESS interconnects the associated subsystems (IVCS, EGIS--CS, CIS, and EDMS) by facilitating the synchronization and delivery of digitized benefits applications, visa issuance and travel notifications, and applicant documentation information between USCIS, CBP, and DoS. EGIS-ESS facilitates the transmission of data between EDMS and multiple subsystems. EGIS-ESS facilitates the data exchange between EDMS and Central Index System 2 (CIS 2),⁶⁵ U.S. Immigration and Customs Enforcement (ICE) Office of the Principal Legal Advisor (OPLA) Case Management System (OCMS),⁶⁶ and USCIS Freedom of Information Act (FOIA) Immigration Records System (FIRST).⁶⁷

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

The EGIS-ESS Support Services includes the:

- **Digitization Notification Service** allows client applications to communicate one Alien Number (A-Number) for an operation and provides the client application with response codes that detail the success or failure of the Digitization Notification Request.
- **Metadata Update Service** transforms the data provided by CIS into the format required by EDMS and places that message on a queue on the ESB 2. The Metadata Update Service also removes any incomplete/invalid dates, (dates with a 00 month, day or year) received by CIS before sending to EDMS.
- **A-File Delivery Service** Data is transmitted securely between OPLA and FIPS and the ESB using Simple Object Access Protocol (SOAP)⁶⁸ Hypertext Transfer Protocol Secure (HTTPS)⁶⁹ and Web Services Security (WS-Security) Headers via this service. HTTPS

⁶⁵See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁶⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF THE PRINCIPAL LEGAL ADVISOR (OPLA) CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-036 (2013 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-ice>.

⁶⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOIA IMMIGRATION RECORDS SYSTEM (FIRST), DHS/USCIS/PIA-077 (2019), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁶⁸ SAOP is a protocol specification for exchanging structured information in the implementation of web services in computer networks.

⁶⁹ HTTPS is an adaptation of the HTTP for secure communication over a computer network.



encrypts the transport and provides server authentication, while usage of the WS-Security Headers will provide client authentication.

Category of Individuals Affected:

Applicants and petitioners seeking immigrant and non-immigrant benefits to include: lawful permanent residents, naturalized citizens, United States border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA).

Information Sharing:

EGIS-ESS facilitates the data exchange between EDMS and USCIS CIS, ICE OPLA, and USCIS FIRST.

Applicable System of Records Notice:

The following SORNs cover the collection, maintenance, and use of EGIS-ESS:

- Alien File, Index, and National File Tracking System,⁷⁰ which covers the collection, use, and maintenance of information related to individuals who have passed through the immigration process. Records maintained in this system of records includes immigration requests forms and supplemental evidence, as well as data in CIS and EDMS; and
- Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System,⁷¹ which covers the processing of record access requests and administrative appeals under the FOIA, as well as access, notification, and amendment requests and administrative appeals under the Privacy Act.

Retention:

EGIS-EDMS System Support Service does not maintain/retain any data. The data is temporarily stored in a queue for a few seconds for processing. Once successfully or unsuccessfully processed, the data is no longer available in EGIS-EDMS System Support Service.

⁷⁰ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁷¹ See DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, 79 Fed. Reg. 6609 (February 4, 2014) available at <https://www.dhs.gov/system-records-notices-sorns>.



Appendix L

EGIS-Verification Service (EGIS-VS)

Background:

The EGIS Verification Service (EGIS-VS) is a service that supports the Employee Eligibility Verification (EEV) program and allows authorized USCIS personnel the ability to search for information against multiple sources via one operation to verify claimed information. The Verification Division application, E-Verify⁷², leverages the EGIS-Verification Service as its automated primary verification process for employee verification. The EEV uses another EGIS service, the EGIS Person Centric Query Service (EGIS-PCQS), as its secondary verification process.

EGIS-VS allows authorized USCIS personnel to search multiple sources for verification information via one operation. The EGIS-VS extracts verification information from USCIS CLAIMS 4,⁷³ ICE Student and Exchange Visitor Information System (SEVIS),⁷⁴ and U.S. Customs and Border Protection (CBP) TECS,⁷⁵ and National Law Enforcement Telecommunications System (NLETS) via the EGIS-NLETS subsystem. The systems and the specific information searched in each are listed below. The unavailability of a certain subsystem does not impact the ability of the EGIS-VIS to return verification information from other subsystems.

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

The EGIS-VS transmits PII and SPII data, such as: first name, last name, date of birth (DOB), Social Security number, naturalization number, passport number, and driver's license number for verification purposes. The following information is exchanged:

⁷² See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>

⁷³ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 4), DHS/USCIS/PIA-015 (2008 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁷⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001 (2020 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-ice>.

⁷⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE, DHS/CBP/PIA-009 (2010 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



USCIS Computer Linked Application Information Management System (CLAIMS 4)⁷⁶

To verify an individual's Naturalization Status, the following data is communicated:

- First name;
- Last name;
- DOB;
- Naturalization number; and
- Social Security number (SSN).

USCIS Redesigned Naturalization Application Casework System (RNACS) via eCISCOR⁷⁷

To verify an individual's naturalization status, the following data is communicated:

- Naturalization Certificate;
- A-Number;
- First name;
- Last name; and
- DOB.

USCIS Central Index System (CIS),⁷⁸ Alien Number Verification module:

To verify an alien registration number, the following data is communicated:

- First name;
- Last name; and
- DOB.

⁷⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 4), DHS/USCIS/PIA-015 (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁷⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁷⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



USCIS Computer Linked Application Information Management System 3 (CLAIMS 3)⁷⁹

To verify a document number, the following data is communicated:

- Alien Number.

USCIS Global⁸⁰

To verify a document number against Global, the following data is communicated:

- A-Number.

U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS)⁸¹

To verify an individual's student visa status, the following data is communicated:

- SEVIS ID.

U.S. Customs and Border Patrol (CBP) Electronic System for Travel Authorization (ESTA)⁸²

To verify password issuance, the following data is communicated:

- First name;
- Last name;
- DOB; and
- Passport number.

CBP Arrival and Departure Information System (ADIS)⁸³

To verify a document number, the following data is communicated:

⁷⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁸⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE Asylum Division, DHS/USCIS/PIA-027(c) (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁸¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001 (2020 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-ice>.

⁸² See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

⁸³ See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM, DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



- Document number;
- Country of issuance;
- Event category; and
- Event count.

National Law Enforcement Telecommunications System (NLETS)⁸⁴ via EGIS NLETS subsystem

To verify the validity of a driver's license, the following data is communicated:

- First name;
- Last name;
- DOB;
- Driver's License number;
- License type;
- License status;
- Address*;
- Physical description*;
- SSN*; and
- Driver's License restrictions (While not an exhaustive list, examples of restrictions could include: driver must wear corrective lenses, driver not to exceed a specific speed limit, a licensed driver 21 years of age or older must be in the front seat, prohibited from nighttime driving.) *.

* NLETS does not prepare a separate response configuration for USCIS so the data elements that are not pertinent (address, physical description, Social Security number, and restrictions) to the verification process will not be stored by USCIS. The address, physical description, Social Security number, and restrictions will not be sent to the audit logs and will never be made available. Further, for increased security measures, the EGIS-VS will strip all data fields and only send a match or no-match response to E-Verify (which is displayed to the E-Verify user).

⁸⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



Category of Individuals Affected:

USCIS uses the EGIS-Verification Service to verify information provided by individuals who interact with USCIS. This includes but is not limited to benefit applicants, petitioners, and derivatives.

Information Sharing:

The EGIS-Verification Service shares information between systems mentioned below:

- USCIS CLAIMS 4;
- USCIS RNACS via eCISCOR;
- USCIS CLAIMS 3;
- USCIS Global;
- USCIS CIS2;
- CBP ESTA;
- CBP ADIS;
- ICE SEVIS; and
- USCIS NLETS.

Applicable System of Records Notice:

The information maintained and shared is covered under the following SORNs:

- Alien File, Index, and National File Tracking System,⁸⁵ which covers CIS, which serves as a DHS-wide index of key information for A-Files (whether paper or electronic). CIS contains information on individuals who interact with DHS. The system contains biographic information on those individuals which can be used to retrieve additional information from other systems. However, A-Files are not contained in CIS;
- Benefits Information System,⁸⁶ which covers the collection and use of immigrant and nonimmigrant benefit request forms and decisional data in CLAIMS 3, CLAIMS 4, and RNACS (via eCISCOR);

⁸⁵ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁸⁶ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.



- Asylum Information and Pre-Screening System,⁸⁷ which covers the collection and use of benefit request forms and decisional data in Global;⁸⁸
- E-Verify Program,⁸⁹ which covers the collection and use of information to verify the information from a driver's license, permit, or state issued ID card if the state has agreed to allow verification of this information through a secure connection between USCIS VIS and NLETS;
- Systematic Alien Verification for Entitlements Program,⁹⁰ which covers the collection and use of information to verify the information from a driver's license, permit, or state issued-ID card if the state has established a MOA with USCIS to allow verification of this information with AAMVA;
- Electronic System for Travel Authorization,⁹¹ which covers the collection and maintenance of individuals who want to travel to the United States under the Visa Waiver Program (VWP), and to determine whether applicants are eligible to travel to and enter the United States under the VWP;
- Arrival and Departure Information System,⁹² which serves as the primary repository for tracking entry and exit data throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes; and
- Student and Exchange Visitor Information System,⁹³ which covers the tracking of certain nonimmigrants and their dependents during their stay in the U.S.

Retention:

The EGIS-Verification Service does not maintain/retain any data. The data is temporarily in queue (a few seconds) for processing. Once successfully or unsuccessfully processed, the data is no longer available in the Verification Service.

⁸⁷ See DHS/USCIS-010 Asylum Information and Pre-Screening, 80 Fed. Reg. 74781 (November 30, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁸⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE Asylum Division, DHS/USCIS/PIA-027(c) (2009 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

⁸⁹ See DHS/USCIS-011 E-Verify Program, 84 Fed. Reg. 28326 (June 18, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁹⁰ See DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records, 85 Fed. Reg. 31798 (May 27, 2020), available at <https://www.dhs.gov/system-records-notices-sorns>.

⁹¹ See DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records, 81 Fed. Reg. 60713 (September 2, 2016) available at <https://www.dhs.gov/system-records-notices-sorns>.

⁹² See DHS/CBP-021 Arrival and Departure Information System (ADIS) System of Records, 80 Fed. Reg. 72081 (November 18, 2015) available at <https://www.dhs.gov/system-records-notices-sorns>.

⁹³ See DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records, 75 Fed. Reg. 412 (January 5, 2010) available at <https://www.dhs.gov/system-records-notices-sorns>.



Appendix M

EGIS-Person Centric Query Service (EGIS-PCQS)

Background:

The EGIS Person Centric Query Service (EGIS-PCQS) is a composite service which allows a system or a person to submit a single query for all transactions involving an immigrant across various USCIS and Department of State (DoS) systems and receive a consolidated and correlated view of the immigrants' past interactions with the government as he or she passed through the U.S. immigration system in response. EGIS-PCQS presents a single access point and eliminates the need to access individual systems separately. EGIS-PCQS does not store data. EGIS-PCQS retrieves and temporarily displays information from connected systems in a consolidated, read-only format for the user.

EGIS-PCQS also includes auxiliary services EGIS-EOIR-Court Schedule, which queries case scheduling information from Executive Office for Immigration Review (EOIR)'s Case Access System (CASE)⁹⁴ for staff information and availability, and USCIS's internal employee COVID-19 contact tracking microservices. EGIS-PCQS does not provide information to EOIR.

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

EGIS-PCQS temporarily displays read-only information from underlying, connected IT systems. The information temporarily displayed from each system varies.

Category of Individuals Affected:

EGIS-PCQS is used to provide a consolidated real-time view of records from multiple systems. EGIS-PCQS allows users to temporarily display real-time data related to an individual such as immigration status, biometric information, and associated biographic information for the purposes of national security, law enforcement, adjudication of applications or petitions for immigration benefits, and border management.

Information Sharing:

EGIS-PCQS retrieves and temporarily displays information from connected systems, which include USCIS systems, DHS systems and external agency systems. These systems include:

USCIS Systems

- Aliens Change of Address Card (AR-11) System;⁹⁵

⁹⁴ The Case Access System (CASE) is the Information Resource Management System that provides the Executive Office for Immigration Review (EOIR) with case tracking and management information, office automation, Internet/Intranet, and automated legal research services. More information is available at <https://www.justice.gov/eoir/major-information-systems>.

⁹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES,



- Benefits Biometrics Support System (BBSS);⁹⁶
- Central Index System 2 (CIS 2);⁹⁷
- Computer Linked Application Information Management System (CLAIMS 3);⁹⁸
- Computer Linked Application Information Management System (CLAIMS 4);⁹⁹
- Customer Profile Management System (CPMS);¹⁰⁰
- Electronic Immigration System 2 (USCIS ELIS);¹⁰¹
- Enterprise Citizenship and Information Services Centralized Operational Repository (eCISCOR);¹⁰²
- FBI Fingerprint and Name Check System (FD258);¹⁰³
- USCIS RAILS;¹⁰⁴

PRIVACY IMPACT ASSESSMENT FOR THE ALIEN CHANGE OF ADDRESS CARD (AR-11), DHS/USCIS/PIA-018 (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁹⁶ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), *available at* <https://www.dhs.gov/system-records-notices-sorns>.

⁹⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁹⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

⁹⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 4), DHS/USCIS/PIA-015 (2008 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM, DHS/USCIS/PIA-056, (2018 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰² See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023 (2009 and subsequent updates), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰³ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), *available at* <https://www.dhs.gov/system-records-notices-sorns>.

¹⁰⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE RAILS, DHS/USCIS/PIA-075 (2018), *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.

- USCIS Global;¹⁰⁵
- Marriage Fraud Amendment System (MFAS);¹⁰⁶ and
- Validation Instrument Business Entity (VIBE).¹⁰⁷

DHS Systems

- DHS National Protection and Programs Directorate (NPPD), Office of Biometric Identity Management (OBIM) Homeland Advanced Recognition Technology (HART);¹⁰⁸
- Customs and Border Patrol (CBP) TECS;¹⁰⁹
- CBP Automated Targeting System – Passenger (ATS-P);¹¹⁰
- CBP Arrival Departure Information System (ADIS);¹¹¹ and
- ICE Student and Exchange Visitor Information System (SEVIS).¹¹²

External Systems

- Department of Justice (DOJ) Executive Office for Immigration Review (EOIR);¹¹³

¹⁰⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE Asylum Division, DHS/USCIS/PIA-027(c) (2009 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016(a) (2008 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE VALIDATION INSTRUMENT FOR BUSINESS ENTERPRISES (VIBE), DHS/USCIS/PIA-044 (2014 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹⁰⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), available at www.dhs.gov/privacy.

¹⁰⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE, DHS/CBP/PIA-009 (2010 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

¹¹⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006 (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

¹¹¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, US CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.

¹¹² See U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001 (2020 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-ice>.

¹¹³ See Justice/EOIR-001 Records and Management Information System, 66 Fed. Reg. 35458 (July 5, 2001).



- Department of State (DOS) Consular Consolidated Database (CCD);¹¹⁴ and
- American Association of Motor Vehicle Administrators (AAMVA) Network Service (AAMVAnet).¹¹⁵

Applicable System of Records Notice:

EGIS-PCQS retrieves and temporarily displays data from other Privacy Act Systems of Record. The source system SORNs (described in the PCQS PIA Appendices) cover the data within EGIS-PCQS.¹¹⁶

Retention:

The EGIS-PCQS subsystem does not maintain/retain any data. The data is temporarily in queue (a few seconds) for processing. Once successfully or unsuccessfully processed, the data is no longer available in EGIS-PCQS.

¹¹⁴ See U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE DoS CONSULAR CONSOLIDATED DATABASE (CCD), available at <https://www.state.gov/documents/organization/242316.pdf>.

¹¹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENTS FOR THE E-VERIFY PROGRAM, DHS/USCIS/PIA-030 (2010 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>. See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM, DHS/USCIS/PIA-006 (2011 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹¹⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



Appendix N

EGIS-Customer Profile Management System Support Services (EGIS-CPMS-SS)

Background:

- The EGIS Customer Profile Management System Support Services (EGIS-CPMS-SS) is the EGIS service that support's USCIS's Customer Profile Management System, which is the repository of biometric & background check data for USCIS.

The EGIS-CPMS-SS within EGIS facilitates communication between Application Support Center (ASC) Biometric Capture stations, the Office of Biometric Identity Management (OBIM) Homeland Advanced Recognition Technology (HART),¹¹⁷ the Federal Bureau of Investigation (FBI) National Name Check Program,¹¹⁸ and the Department of Defense (DoD) Automated Biometric Identification System (ABIS)¹¹⁹ with USCIS's Customer Profile Management System (CPMS).¹²⁰

Through the EGIS-CPMS-SS, USCIS sends both biographic and biometric information related to DoD to conduct fingerprint checks on individuals seeking refugee or asylum protections as well as their eligible family members. USCIS, via EGIS-CPMS-SS, sends the benefit requestor's date of birth, country of birth, race, ethnicity, weight, height, eye color, hair color, gender, address, and biometric images (i.e., fingerprints, photograph, and signature) to DoD in order to conduct the fingerprint background check. The DoD fingerprint check is an image-based search of the DoD's ABIS.¹²¹ ABIS contains DoD encounter history information compiled during its operations and from individuals seeking access to its installations. USCIS only sends fingerprints to ABIS for specific benefit types when the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military. Currently, those specific benefit types are refugee, asylum, and international relative petitions related to those benefit types.¹²² DoD responds to the fingerprint check with either a "Non-Match" or "Match" response. A Non-Match response means that DoD has no encounter history information related to the fingerprints submitted by the benefit requestor. A Match response means DoD had obtained fingerprints from

¹¹⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

¹¹⁸ The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI). See DOJ/FBI-002 Central Records System (CRS), 66 Fed. Reg. 29994 (June 4, 2001).

¹¹⁹ Department of Defense Detainee Biometric Information System, 72 Fed. Reg. 14534 (March 28, 2007).

¹²⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹²¹ Department of Defense Detainee Biometric Information System, 72 Fed. Reg. 14534 (March 28, 2007).

¹²² DoD retention of these biometrics varies based on benefit type.



the same individual who had submitted fingerprints to USCIS. Match responses are accompanied by pertinent text explaining the nature of the previous DoD encounter.

USCIS sends immigration requestor information to the FBI to conduct name checks through EGIS-CPMS-SS. All FBI Name Check requests, responses, and queries flow through the EGIS-CPMS-SS; there is no direct connection between the FBI systems and CPMS.

The FBI Name Check is a name-based search of the FBI's Central Records System (CRS) and Universal Index (UNI).¹²³ CRS contains FBI investigative, administrative, criminal, personnel, and other files compiled for law enforcement and national security purposes. UNI consists of administrative, benefit requestor, criminal, personnel, and other law enforcement files. The FBI responds to the FBI Name Check with either a: "no record," "positive response," or "pending." A no record response means that the FBI has no relevant information based on the name and DOB of the benefit requestor. A pending response means further research is needed before the FBI can provide a final response. For those records with an initial response of pending, the FBI will complete a review of its records and provide a final response of no record or positive response. A positive response means the FBI has information relating to the subject, which is obtained by USCIS officers through separate processes outside of CPMS.

USCIS simultaneously sends benefit requestor information to include, name, DOB, country of birth, race, gender, address, and biometric images, (including photographs and fingerprints) to both IDENT and FBI Next Generation Identification (NGI) in order to conduct the fingerprint background check.¹²⁴ NGI contains FBI criminal history record information compiled from law enforcement and national security submitters. The FBI fingerprint check is an image-based search of NGI. The FBI responds to the fingerprint check with either a: "Non-Match," "Match," or unclassifiable. A Non-Match response means that the FBI has no criminal history information related to the fingerprints captured from the benefit requestor. A Match response means the FBI has criminal history information relating to the fingerprints submitted. A Match response is usually accompanied by the Identity History Summary, previously known as the Record of Arrest and Prosecution Sheet (RAP Sheet). An unclassifiable response means the fingerprint image quality was too poor to compare against fingerprint records contained within IDENT and NGI. For those records with an initial response of unclassifiable, USCIS captures and submits additional fingerprints to obtain a valid response.

¹²³ See DOJ/FBI-002 Central Records System (CRS), 66 FR 29994 (June 4, 2001).

¹²⁴ The FBI replaced its Integrated Automated Fingerprint Identification System (IAFIS) with the Next Generation Identification (NGI). Please see the Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability for more information, available at <https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngiinteroperability-1>.



The EGIS-CPMS-SS supports the information sharing exchange of biometric data collected at the ASCs for biometric processing of immigration applicants.¹²⁵ This also includes data from produced immigration benefit cards to USCIS government partners (e.g., OBIM). EGIS-CPMS-SS also facilitates the exchange of document information required by all case management systems in USCIS to produce benefit documents as well as notices sent to applicants.

EGIS-CPMS-SS also facilitates the exchange of biometrics (e.g., fingerprints, photograph, and/or iris) along with basic biographic data (e.g. name, date of birth, place of birth, and gender) information collected from the UNHCR to OBIM HART. DHS and UNHCR entered into an MOU to conduct a pilot to share refugee data. As part of the pilot, DHS and UNHCR are expanding the biometric information UNHCR shares with refugee processing stakeholders (e.g., DHS CBP and USCIS and DoS). This information allows USCIS verify whether the individual being processed by USCIS for possible refugee resettlement is the same individual who was registered and referred by UNHCR.¹²⁶

EGIS-CPMS-SS facilitates the exchange of information between UNCHR and OBIM IDENT. UNHCR is sharing biometric and biographic information related to individuals seeking admission into the USWRAP program. The transfer of data is accomplished using EGIS-CPMS-SS. Upon receipt, EGIS-CPMS-SS forwards the information to OBIM IDENT where it is retained. EGIS-CPMS-SS only facilitates the exchange of information from UNHCR and OBIM IDENT. USCIS does not retain or retrieve the records using a unique personal identifier. Therefore, SORN coverage is not required for this exchange of information.

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

- **Application Support Center (ASC) Biometric Capture Stations:** The data will be a one-way transfer of captured 10-print biometric and biographic data of immigration petitioners that will be sent to the ESB 2 for business processing across various DHS systems such as USCIS CPMS, OBIM HART, and USCIS ELIS.¹²⁷

¹²⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE (CPMS), DHS/USCIS/PIA-060 (2015 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹²⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES (UNHCR) INFORMATION DATA SHARE, DHS/USCIS/PIA-081 (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.

¹²⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM, DHS/USCIS/PIA-056, (2018 and subsequent updates), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



- **UNHCR:** The data will be a one-way transfer of refugee biometric data (e.g., fingerprints, photograph, and/or iris) along with basic biographic data (e.g. name, date of birth, place of birth, and gender) from UNHCR to OBIM HART.
- **OBIM HART:** Through EGIS-CPMS-SS, CPMS also sends fingerprints, photographs, and limited biographic information to the OBIM HART.¹²⁸

Category of Individuals Affected:

Most individuals who have filed immigration requests for themselves or on the behalf of others (i.e., immigration requestors and beneficiaries) are subject to background, identity, and security checks to ensure eligibility for the requested benefit and to ensure that they do not pose a threat to public safety or to the national security of the United States. Other individuals in connection with immigration requests or other requests may also be subject to certain background, identity, and security checks.

Information Sharing:

USCIS uses EGIS-CPMS-SS to share biometric data collected at the ASC to verify identity and to conduct background checks of immigration applicants. This data is shared across various DHS systems such as USCIS CPMS, OBIM HART, and USCIS ELIS. In addition, EGIS-CPMS-SS facilitates communications with UNHCR, DOJ FBI Name Check¹²⁹ and DoD ABIS.¹³⁰

Applicable System of Records Notice:

The collection, use, maintenance, and dissemination of information is covered under the following system of records notices:

- Immigration Biometric and Background Check,¹³¹ which covers the collection, use, and storage of biometric and biographic data for background checks and its results.
- External Biometric Records,¹³² which discusses the use of biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement,

¹²⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim>.

¹²⁹ See DOJ/FBI-002 Central Records System (CRS) System of Records, 66 Fed. Reg. 29994 (June 4, 2001).

¹³⁰ See Department of Defense Detainee Biometric Information System System of Records, 72 Fed. Reg. 14534 (March 28, 2007).

¹³¹ See DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹³² See DHS/USCIS-041 External Biometric Records, 83 FR 17829 (April 24, 2018).



intelligence, and national defense. This SORN specifically covers the exchange of information from UNHCR to OBIM.

Retention:

The EGIS CPMS-SS subsystem does not maintain/retain any data. Usually the data is temporarily retained/ remains in memory (queue) for few seconds awaiting transmission. Sometimes the data remain in the queue for 24-48 hours; this is in the case if data is not picked up by the processing system due to some issue experienced by the recipient. Once the data is successfully received by the recipient system, it is deleted from EGIS-CPMS-SS.



Appendix O

EGIS-American Association of Motor Vehicle Administrators (AAMVA) Hub Services (EGIS-AHS)

Background:

The EGIS American Association of Motor Vehicle Administrators (AAMVA) Hub Services are a collection of interfaces and business logic that facilitates the transmission between AAMVA and multiple USCIS sub systems. The EGIS AAMVA Hub Service (EGIS-AHS) Subsystem facilitates the secure connection between USCIS Verification Information System (VIS) and American Association on Motor Vehicle Administrators (AAMVA) in support of the Systematic Alien Verification for Entitlements (SAVE).

The SAVE Photo Matching Tool is available for a participating Motor Vehicle Association (MVA) to access the SAVE system through the American Association of Motor Vehicle Administrators Network (AAMVAnet). The Photo Matching Tool is a process whereby an MVA employee submits a query to SAVE for verification of an individual's status using the USCIS-issued Permanent Resident Card or Employment Authorization Card that an applicant presents to MVA personnel.

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

A MVA employee is able to submit a query to SAVE for verification of an applicant's immigration status using the USCIS-issued identification card that an individual presents to MVA personnel. SAVE retrieves and displays the individual's information, including a photograph from CPMS to allow the MVA employee to determine if the information and photograph displayed in SAVE via CPMS matches the information the applicant presented to MVA personnel.

Category of Individuals Affected:

The EGIS-AHS subsystem supports SAVE. The MVA administrators uses SAVE to verify a USCIS-issued identification card.

Information Sharing:

EGIS-AHS provide an electronic interface between VIS and AAMVA.

Applicable System of Records Notice:

The collection, use, maintenance, and dissemination of information is covered under the following system of records notice:

- Systematic Alien Verification for Entitlements (SAVE) Program,¹³³ which covers the collection and use of information to verify the information from a driver's

¹³³ See DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records, 85



license, permit, or state issued ID card if the State has established a MOA with DHS USCIS to allow verification of this information.

Retention:

EGIS-AHS service does not maintain/retain any data. The data is temporarily in queue (a few seconds) for processing. Once successfully or unsuccessfully processed, the data is no longer available in EGIS-AHS.



Appendix P

Third Party Integration (3PI)

Background:

Third-party Application Integration (3PI) that will enable third parties, such as attorneys, accredited representatives, and community-based organizations who use a third-party case management software system to maintain their clients' applicant data to submit applications electronically, directly from their software, instead of mailing paper applications to the Lockbox. 3PI will act as the single electronic gateway for third party software providers to do business with USCIS and serve as a conduit for the intake and validation of applicant data, which will then be stored in USCIS case management systems.

Current Environment

To reach the next level of advancement in electronic filing (e-filing), consideration is being given to attorneys, accredited representatives, community-based organizations and others who use a third-party case management software system. Case management software systems are used by many organizations in order to compile, organize and manage their client data within a digital platform prior to submission to USCIS. In the existing third-party flow, the applicant keys information into the third party's case management system and evidence is scanned and uploaded into their system. To get this data to USCIS, the representative using the third-party case management software must either print the information on paper USCIS forms and mail it to the Lockbox or directly key each field, one for one, into myUSCIS (duplicating data entry). Because these systems are capable of automating user data onto paper forms and not into myUSCIS, a large population of filers continue to submit paper applications to USCIS through the Lockbox¹³⁴. Roughly 3 percent of representative filings come in through myUSCIS. This new electronic interface, referred to as Third Party Application Integration or "3PI," will provide third-party vendors the ability to submit applications electronically, directly from their software, instead of mailing paper applications to the Lockbox.

3PI Pilot Project

3PI will provide a set of simple to use Application Programming Interfaces (APIs) based on modern, lightweight and open standards. The APIs and associated documentation required to build applications will be hosted on the developer portal, a USCIS website (Under development, but on the uscis.gov site), which will require a USCIS account to access. The electronic interface

¹³⁴ A Lockbox is a secure facility used by government agencies and private organizations to facilitate the collection and deposit of fees. The Department of Treasury designated a financial agent to perform Lockbox services for USCIS. The Lockbox service provider manages the intake of USCIS benefit applications and the collection of associated fees submitted directly by mail. The Lockbox service provider does not approve or deny petitions/applications received.



will be protected with industry standard security and federally required protocols ensuring proper authentication and authorization of the consumers, as well as maintaining the integrity and confidentiality of the data. Any developer doing business with USCIS, will be required to create an account and request an access token to move their application into the production environment to send live data. The developer will have to demonstrate that they have built and tested a successful application in the test environment and will have to demonstrate that the application has a 99% success rating based on the established USCIS sandbox metrics. All traffic in the testing and production environments is tracked using the Apigee API management platform. This will enable USCIS to see every single transaction the entity does while within the USCIS environment. Hosted in a modern cloud-based environment with auto scaling capabilities ensures a high level of availability and performance characteristics, which would give USCIS more accurate and secure metrics behind who is filing with USCIS.

3PI will act as the single electronic gateway for third-party software providers to do business with USCIS. It will serve as a conduit for intake of validated applicant data, which will be stored in USCIS case management systems such as ELIS and CLAIMS 3. USCIS will validate the applicant data before the data comes into the USCIS system. To do this USCIS is leveraging asynchronous API calls. When a submission is started, the validation of the data is first performed. This validation checks for required fields and preclusion fields formatted exactly how USCIS dictated based on agreed upon requirements used across myUSCIS and the current intake methods at USCIS Lockbox locations.

Once the applicant data and evidence has been validated and uploaded in a draft form, the USCIS payment service will enable the payment of any required fees. Payment is made using the U.S. Department of Treasury's Pay.gov service. USCIS does not collect the fee directly. Rather, the individual is redirected to the Pay.Gov interface by the USCIS payment service, and Pay.gov collects payment information (e.g., credit card, debit card, or Automated Clearing House (ACH debit)) from a personal bank account and billing information. Once Pay.Gov validates the payment information, the account holder is routed back to USCIS. The payment service communicates directly with Pay.gov and a unique URL is passed back to the user to submit to USCIS. This is the same payment service and process currently used by myUSCIS Account experience when an individual submits a forms/payment.

The details of which system processes a filing type will not be visible to third parties. This interface will operate in a one-way stream and only allow the ingestion of validated payloads. No other communication or information will be passed back to the client besides a transmission status message (transmission complete/incomplete), which includes a receipt number. All other communications will remain business as usual from USCIS in the form of paper notifications or through the applicant's USCIS account if they choose to create one using the myUSCIS Account Experience (<https://myaccount.uscis.dhs.gov/>).



USCIS has identified two use cases that will interact through the 3PI channel

- 1.) A developer, on behalf of a third-party software system, building an application to do business with USCIS. This user is not submitting applications, rather they are interacting with 3PI to solely build their application. (Note: No PII is involved in this Use Case); and
- 2.) A representative/user who is using the third-party software application integrated with 3PI and is filing on behalf of an applicant. (Note: PII is involved in this Use Case).

3PI Use Case #1

For the first use case, a developer will navigate to the 3PI Developer Portal. The Developer Portal is the front facing piece of USCIS' API management platform. USCIS is using a software called Apigee for its API management platform. This software currently has an ATO and is being used by the agency today. This platform provides all the securities and administrative controls for the 3PI managers to expose APIs and control access to all information related to 3PI. A link to the portal will be found on the uscis.gov site, which is being coordinated through the External Affairs Directorate (EXA).

When the developer arrives at the developer portal, they will be met with a home screen welcoming the developer to the 3PI developer portal and prompting the developer to create a USCIS account through myUSCIS Account Experience (myAccount), utilizing Security Assertion Markup Language (Saml) authentication. Once the developer has created an account, the Apigee platform will allow the developer to access the technical documentation for the individual USCIS APIs needed to build their application within the portal. In addition, the developer will be able to request an access token to gain access to the sandbox environment. The developer application will not be able to interact with any of the USCIS systems without an access token.

The sandbox environment is a testing environment isolated from all USCIS production systems, where developers can test the code for their application. 3PI Sandbox will be hosted in a Staging Environment. Internal USCIS users will be authenticated to Identity Credential and Access Management (ICAM) for access to the Portal. External Users are required to have an Accounts Public credentials to be authenticated for access to Portal & APIs. The Developer applications using the 3PI Products will access the APIs secured using OAuth2.0 protocol. The OAuth tokens are valid for 30 minutes at a time and have to renewed for continued access. Apigee's in-built features provides data protection, threat detection, access control, identity management and governance. All 3PI components (Apigee, Portal and the Middleware-product) are hosted in Amazon Web Services (AWS).

Based on the documentation provided by USCIS, the developers will use the sandbox to build and test their application. USCIS will not interact with the developers as they are creating their individual applications. USCIS will publish the specifications for the developer to build their application. The developer will then build their application based on these specifications. When



the developer is ready, they can request approval for access to the production environment. This will be the first direct interaction between USCIS and the developer.

This production environment access request is sent to the API management team, which will consist of the members from Office of Intake & Document Production (OIDP) and Office of Information Technology (OIT). The developer application will be vetted based on technical metrics through test cases and data gathered from interactions within the sandbox through the Apigee platform.

The Apigee platform has its own user management module. Each user tier can be managed to have different limitations as far as consumption quota limits and API Products they are allowed to integrate with. All users start in the sandbox environment. Usage will be tracked and access revoked/blocked/limited by Apigee admins based on the metrics being tracked. Some examples of these metrics include, API call success rate, API call failure rate, the total rate of calls and the total amount of calls. Based on these metrics USCIS will be able to assess the viability and performance of an application being developed by the third-party developer. To request production access, the developer's application will be assessed upon the data gathered by the Apigee platform. The developer application will have to demonstrate a 98% success rate to be approved for production access.

Once the developer is approved, the Apigee platform will issue the developer a client key and a secret. The client key and secret will be used each time the third-party application interacts with the 3PI APIs. Every time the third-party application makes a call to any of 3PI APIs, the client key and secrets are verified by Apigee and an access token will be generated and sent back to the third-party application. That access token is what will allow the third-party application access to the 3PI backend server for submission. The access tokens are short lived and will only remain valid for a maximum of 30 minutes. After this point, the third-party software system will have to request a new access token. This interaction happens seamlessly within the Apigee API management platform.

All developer applications will be the property of the third-party vendor. The third-party vendor will be responsible for selling, providing and managing their own application to their client base for them to use. USCIS will not be involved in the sale of licenses, permissions or access to these applications.

3PI Use Case #2

The second use case comes from the perspective of a representative/user filing on behalf of an applicant. In this use case, the representative is using a third-party case management system to manage their client's data. The third-party case management system has been integrated with USCIS via the 3PI application developed by a vendor using the pathway described above. When the representative is ready to file, they will select to execute a function on their software which



will call the 3PI APIs, starting by acquiring an access token as describe above. The validation and payment processes described in Use Case #1 apply to this use case.

To start, all the PII information is collected and stored in the third-party case management system. It's the representative's duty to ensure that all the required data has been gathered on their end, otherwise no submission will occur. 3PI only provides a pathway for data to enter USCIS systems. It does not create nor manage a user interface; this is done through the third-party software application.

When the representative is ready to file, the third-party software system will "package" the form data and evidence and make four asynchronous calls to four external facing APIs through the 3PI channel, which is hosted in AWS through the EGIS boundary. The full payload consisting of the form data, evidence, and evidence of payment from Pay.gov will be dropped on the ELIS queue, where ELIS will ingest the payload. This queue is the same queue the lockbox¹³⁵ uses, and the payloads will be functionally identical.

Below describes the API flow through the 3PI channel. There are a total of four APIs. The API calls are what will drive the submission from the third-party case management system to USCIS systems. The API flow is described below in sequential order.

1. **"form/submit/start" API** - This is the first API call that the third-party case management software will make. This API will validate the JSON data (form data) requirements, encrypt the JSON, store it in the EGIS Draft Storage container and send back a unique transaction ID to the third-party case management system. The transaction ID will be used later to submit evidence and payment. It links all parts of a single submission together. The draft storage container will only hold data for 48 hours maximum. After that point the data is automatically deleted. The JSON data will remain in the EGIS draft storage container until payment is made (later described) or the 48hours window has hit. If the 48 hours window has expired, the data is deleted and the application will have to start over again. In essence, the representative submitting through the third-party channel has 48 hours to complete payment.
 2. **"forms/submit/evidence" API** – This is the second call the third-party case management software will make. After a successful call to the "form/submit/start" API, the "form/submit/evidence" API will make a rest API call to ELIS to store the evidence directly in ELIS draft storage. Unlike the initial forms draft, the evidence is not stored in EGIS draft storage.
-



3. **“forms/submit/Complete” API** – This API is the third API call that is responsible for retrieving the payment amount for the form, sending a unique Pay.gov URL and Agency Tracking ID back to the representative and ultimately submitting the full payload, consisting of the form data JSON supporting evidence and payment onto the ELIS queue. Again, this is all linked through the transactions IDs that are created with the call to the first API (forms/submit/start).
4. **“form/submit/status” API** – This is the final API in the submission process for 3PI. This API will take the transaction ID and make an internal rest API call to ELIS’ Receipt Number Service. The receipt number will then be passed back to the user, as well as the case status, using the CRIS service API.

The four APIs explained above are responsible for driving a completed submission through the 3PI channel. While APIs are called in a sequential order, it is important to note that these processes happen almost instantaneously when the end user is ready to submit. The data is stored and maintained externally in the third-party case management system. When the user is ready to submit an application, the above APIs are called to process and pass the payload through to ELIS. The triggering event for ultimate submission will come when the user has made payment through Pay.gov. If the user does not make payment within the 48-hour window (EGIS draft storage time limit), then they will have to start a new submission, which on their end will be another click of a button within their case management software.

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

Since this is another gateway for form intake at USCIS, 3PI collects information that includes names, addresses, email addresses and other specific filing information based on the USCIS form type. During the 3PI pilot phase the following forms will be submitted via 3PI:

- Form I-90.

3PI transmits the form information from the third-party case management system to the applicable USCIS case management system (USCIS ELIS). As additional USCIS forms are made available for submission via 3PI, USCIS will update this Appendix.

Category of Individuals Affected:

3PI relates to cases where third-party actuaries are assisting individuals applying for, updating, and processing citizenship and immigration requests. USCIS will use the data received through the 3PI channels to intake immigration requests. USCIS will then use the information received to process, review, and adjudicate immigration benefits in the applicable USCIS case management system. The use of 3PI does not otherwise change the process for filing, processing and adjudicating immigration requests.



Information Sharing:

The purpose of 3PI is to serve as an intake channel for USCIS immigration forms. To enable this, 3PI will provide a connection to multiple third-party case management systems. 3PI third party vendors will be vetted based on technical requirements and business requirements. The vendors will have to request production access for any 3PI exposed API, where USCIS will vet the vendor based on technical requirements and test cases, as well as, a business questionnaire interview and signed access agreement.

Applicable System of Records Notice:

SORN coverage is provided by the following:

- Alien File, Index, and National File Tracking System of Records¹³⁶, which covers the collection, use, and maintenance of benefit requests forms and supplemental evidence;
- Benefits Information System¹³⁷, which covers the collection and use of immigrant and nonimmigrant benefit request forms, decisional data, and associated fees for adjudication; and
- E-Authentication Records System of Records,¹³⁸ which covers how DHS collects information in order to authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application.

Retention:

3PI payloads including immigration benefit form data and evidence uploads, can only be stored in the EGIS draft case container for up to 48 hours. The USCIS case management systems receiving the data via 3PI will retain the data based on the applicable retention schedule. USCIS will work with the Records Office to determine the applicable records schedule.

¹³⁶ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹³⁷ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹³⁸ See DHS/ALL-037 E-Authentication Records System of Records, 79 Fed. Reg. 46857 (August 11, 2014), available at <https://www.dhs.gov/system-records-notices-sorns>.



Appendix Q

EGIS-Security Center Operations Intake Service (EGIS-SCOPS)

Background:

USCIS EGIS-SCOPS Intake provides a bridge service, which enables electronic connection and messaging from USCIS SCOPS Applicant Service Centers (ASC) providers (i.e., California, Nebraska, Texas, Vermont Service Center) to the backend consuming Information Technology systems.

The backend systems currently consist of the USCIS Electronic Document Management System (EDMS), which is the USCS system of records, that stores the scanned PDF case image files (i.e. I-129 forms submitted from the ASCs), and the DoS Kentucky Consular Center (DoS KCC) for adjudicating the Non-Immigrant workers' Visa entries to the United States. EGIS-SCOPS performs all legacy operational business functions and augments the received case files as part of their adjudication process. This service also provides secure file messaging services between USCIS and DoS systems.

USCIS EGIS-SCOPS Intake service is currently undergoing a modernization effort in response to two USCIS mandates due 2/2020. These mandates comprise of 1- all the agency applications and services to move their development and operations out of the DHS Next Generation Data Center1 (DHS NGDC DC1) and into the Amazon Web Service (AWS) Cloud, and (2) all the agency applications and services to move away from using the TIBCO technology stack due to its' 2/2020 licensing expiration. The EGIS-SCOPS Intake Service provides support to the USCIS eProcessing initiatives by:

1. Electronically receiving and validating the scanned adjudicated I-129 Case Transaction PDF Image files from SCOPS ASCs; and
2. Sending them to the downstream EDMS and DoS KCC systems per requirements.

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

The entire process flow is triggered by the SCOPS Service Center Operators, who are the Producers of the immigration benefit PDF case image files. The sequence of entire process flow steps are described below:

1. The SCOPS ASC operator scans paper copies of the I-xxx immigration benefit case files (i.e., I-129s);
2. The SCOPS ASC operator will then perform QA on the resulting scanned PDF Image case file (i.e., remove blank pages or remove duplicate pages) via the desktop PC connected to the Scanner;
3. Once the operator is satisfied with the QA results, he/she will store the QA'd scanned PDF



Image case file on a directory mapped to an NFS Mount Share which is accessible to the EGIS SCOPS Intake Service;

4. The EGIS SCOPS Intake Service will receive the scanned PDF image files from the SCOPS ASCs Mount Share, will perform validation checks on them, and will query eCISCOR database to retrieve metadata associated with the scanned PDF Image Case file which is required by EDMS;
5. If the scanned PDF case image file passes all EGIS validation, then the EGIS SCOPS Intake Service will zip both the scanned PDF case image file as well as associated metadata to a zipped file and store it on the EDMS NFS Mount Share;
6. The EGIS SCOPS Intake Service will then pass the URL address of the zipped file for EDMS to retrieve;
7. The EDMS system:
 - 7.1 Makes an https call using the URL provided by EGIS SCOPS Intake Service to access the zipped file containing both the scanned case PDF Image file as well the XML data file and validates it; and
 - 7.2 If file validation successful, the EDMS system will store the message. Else it will send an error back to the EGIS SCOPS Intake Service;
8. The EGIS SCOPS Intake Service also encrypts the scanned image file for DoS KCC transmission and sends the encrypted file to the DoS NFS Mount Share;
9. The USCIS SnapMirror technology periodically picks up these messages from DoS NFS Mount Share and electronically sends them to the DoS SnapMirror for DoS Ingestion;
10. The EGIS SCOPS Intake Service performs cleanup of messages from both its' EDMS and DoS NFS Shares, which are at least 3 days old and have already been successfully ingested by EDMS; and
11. The EGIS SCOPS Intake Service subsequently repeats the steps above to process the next SCOPS scanned message.

Category of Individuals Affected:

Reference Data is not related to specific individuals, but serves as a standardized repository for consistent data element enumeration.

Information Sharing:

THE EGIS SCOPS subsystem transfers data between USCIS eCISCOR, EDMS, SCOPS ASCs, and US DoS KCC.



Applicable System of Records Notice:

The following SORNs cover the collection, maintenance, and use of SCOPS:

- Alien File, Index, and National File Tracking System,¹³⁹ which covers the petition, supplemental evidence, and decision notices;
- Fraud Detection and National Security Records,¹⁴⁰ which covers the cases referred to CFDO for administrative inquiry and identified as benefit fraud; and
- Benefits Information System,¹⁴¹ which covers the review of applications and petitions

Retention:

The SCOPS subsystem does not permanently maintain/retain any data. The data is temporarily in queue for processing. Encrypted archive files are retained until transfer verification is complete, and once successfully or unsuccessfully processed, the data is no longer available in the SCOPS subsystem.

¹³⁹ See DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹⁴⁰ See DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 Fed. Reg. 47411 (August 8, 2012), available at <https://www.dhs.gov/system-records-notices-sorns>.

¹⁴¹ See DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.



Appendix R

EGIS-National Law Enforcement Telecom System (EGIS-NLETS)

Background:

In support of the E-Verify Program, USCIS established a secure connection between USCIS VIS and NLETS to verify information related to individual's drivers licenses, drivers permits, and state-issued identification (ID) cards. In ESB2 these processes were contained in the VIBE and VS subsystems, EGIS has compartmentalized this in a single separate subsystem, EGIS-NLETS.

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

To verify the validity of a driver's license, the following data is communicated:

- First name;
- Last name;
- DOB;
- Driver's License number;
- License type;
- License status;
- Address*;
- Physical description*;
- Social Security number*;
- Restrictions*.

* NLETS does not prepare a separate response configuration for USCIS so the data elements that are not pertinent (address, physical description, Social Security number, and restrictions) to the verification process will not be stored by USCIS. The address, physical description, SSN, and restrictions will not be sent to the audit logs and will never be made available. Further, for increased security measures, the EGIS-NLETS will strip all data fields and only send a match or no-match response to E-Verify (which is displayed to the E-Verify user).

Category of Individuals Affected:

USCIS uses the EGIS-NLETS subsystem to verify information provided by individuals who interact with USCIS. This includes but is not limited to benefit applicants, petitioners, and derivatives.

Information Sharing:

The EGIS-NLETS subsystem transfers data between the NLETS maintained by US DOJ, EGIS-VS, and EGIS-PCQS subsystems

Applicable System of Records Notice:

SORN coverage is provided by the following:



- E-Verify Program,¹⁴² which covers the collection and use of information to verify the information from a driver's license, permit, or state issued ID card if the state has agreed to allow verification of this information through a secure connection between USCIS VIS and NLETS.

Retention:

The EGIS-NLETS subsystem does not permanently maintain/retain any data. The data is temporarily in queue for processing. Messages are retained until they are consumed or expire, and once successfully or unsuccessfully processed, the data is no longer available in the EGIS-NLETS subsystem.

¹⁴² See DHS/USCIS-011 E-Verify Program, 84 Fed. Reg. 28326 (June 18, 2019), available at <https://www.dhs.gov/system-records-notices-sorns>.