Privacy Impact Assessment

for the

Automated Real-Time Identity Exchange System (ARIES)

DHS Reference No. DHS/OBIM/PIA-006

July 15, 2022

Homeland Security

Abstract

The Automated Real-time Identity Exchange System (ARIES) technology enables a single user interface for the facilitation of current international fingerprint-based information sharing programs by the U.S. Department of Homeland Security (DHS), U.S. Department of State (DOS), U.S. Department of Defense (DoD), and U.S. Department of Justice (DOJ) with foreign partners. The ARIES technology facilitates connectivity and bilateral data exchange between foreign partners and domestic U.S. government agencies and improves auditing of fingerprint-based information sharing programs. ARIES provides a technical pathway to access the DHS Automated Biometric Identification System (IDENT) and IDENT's replacement biometric system, Homeland Advanced Recognition Technology (HART). The Office of Biometric Identity Management (OBIM) is publishing a Privacy Impact Assessment (PIA) because ARIES allows the Department to access and share biometric data, associated biographic data, and encounter data.

Overview

The U.S. Government works with foreign partners to increase cooperation in international information sharing. OBIM's new technology, ARIES, supports fingerprint-based information sharing for the purposes of enhancing and encouraging cooperation for the effective administration and enforcement of criminal and immigration laws and increasing public security. ARIES provides a user interface for biometric identity information exchange between the United States and applicable foreign partners using current DHS security standards, proper formatting of encounter submissions for the applicable U.S. Government systems, and message routing. ARIES implements the IDENT/HART business rules, which determine what information is sharable and what is not. IDENT, and not ARIES, performs the biometric matching.

At the present time, the U.S. Government is sharing information based on fingerprint-based data exchange. ARIES supports several biometrics-based programs, such as the International Biometric Information Sharing Program (IBIS),[1] the Biometric Identification Transnational Migration Alert Program (BITMAP),[2] and the U.S. Immigration and Customs Enforcement (ICE)

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASESSMENTS FOR THE DHS INTERNATIONAL BIOMETRIC INTEROPERABILITY INITIATIVE FOR THE VISA WAIVER PROGRAM, DHS/ALL/PIA-089 (2020) *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[2] BITMAP is a comprehensive information-sharing program, designed to strengthen the international cooperation and coordination of law enforcement agencies' efforts to combat transnational criminal activity, enhance border security, and enforce customs and immigration laws. BITMAP leverages biometric and biographic information collected and shared by foreign partners, logistically capable of identifying foreign nationals within the host country's geographic borders reasonably suspected to be or involved in criminal activity that poses an immigration, criminal, or international security risk. The forthcoming BITMAP PIA will analyze how ICE uses biometric and biographic data and describe the exchange of information between ICE and its law enforcement partners, in a manner that safeguards legal rights, civil liberties, and privacy rights in accordance with law, regulation, and policy.

Criminal History Information Sharing Program (CHIS),[3] and may support other fingerprint-based information sharing programs in the future. These programs bolster international security by sharing personal information for the purposes of counterterrorism, disrupting transnational organized crime, and reducing illegal immigration. DHS and its Components have developed PIAs for the programs supported by ARIES.

The ARIES infrastructure and user interface will replace the current DHS gateway, run through CBP, for biometric based submissions for all internationally based programs that currently use DHS IDENT/HART[4] as the primary conduit for biometric data exchange.

ARIES Functionality

ARIES is a technologically advanced infrastructure and user interface that supports fingerprint-based information exchange between the DHS, DOS, DoD, DOJ, and foreign partners. ARIES can be scaled to support information sharing based on other biometric modalities as they may be supported by agreements and policies in the future. The Office of Biometric Identity Management, in conjunction with U.S. Government partners, intends to use ARIES to establish connectivity with CBP's Automated Targeting System (ATS) Unified Passenger (UPAX),[5] IDENT/HART, DOJ's Next Generation Identification (NGI),[6] and the DoD's Automated Biometric Identification System (ABIS),[7] for the facilitation of such identity information exchanges.[8] Since DOS does not have a fingerprint-based system, its data is maintained and exchanged through IDENT/HART. The ARIES information exchange infrastructure has been

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID) CRIMINAL HISTORY INFORMATION SHARING (CHIS) PROGRAM, DHS/ICE/PIA-015, *available at* https://www.dhs.gov/privacy-documents-ice.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENTS FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), and AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT 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.

[6] *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENTS FOR VARIOUS USES OF FBI'S NEXT GENERATION IDENTIFIER SYSTEM, *available at* https://www.fbi.gov/services/ information-management/foipa/privacy-impact-assessments.

[7] See *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activities,* January 2016 Update, on file with the DHS Privacy Office.

[8] As biometric information sharing programs develop, the intention is for ARIES to be able to broker a search of other systems (e.g., DoD ABIS, DOJ NGI) to adhere to current agreements. ARIES is the technology that allows for the connectivity and data exchange to occur. This PIA will be updated should any additional biometric information sharing programs connect to ARIES as part of the data exchange process.

developed in accordance with the DHS 4300A Sensitive Systems Handbook,[9] which provides implementation criteria for the rigorous requirements mandated by DHS's information security program.

ARIES has three main components for fingerprint-based information sharing: (1) biometric and associated biographic data exchange infrastructure; (2) an administrative application used for onboarding, changing user configurations, and reporting; and (3) a U.S. Government user interface for reviewing identity information.

Data Exchange

ARIES acts as a technical pathway to transfer information. ARIES translates and reformats incoming biometric[10] submissions to search designated U.S. Government biometric repositories (e.g., DHS IDENT/HART,[11] DoD Automated Biometric Identity System,[12] CBP Automated Targeting System Framework UPAX,[13,14] and DOJ FBI Next Generation Identification[15]) in a readable format for the Department and other U.S. Government users' available technology. These readable formats include DOJ/DoD Electronic Biometric Transmission Specification (EBTS), DHS IDENT Exchange Messages (IXM),[16] National Institute of Standards and Technology (NIST), National Information Exchange Model (NIEM), and JavaScript Object Notification (JSON). The ARIES technical pathway infrastructure is also able to translate limited, fixed value filtered text responses into the native language of the submitter without human review (e.g., Spanish). As part of the gateway, OBIM manages business rules[17] for the transmission of

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

[10] Currently, DHS receives fingerprints, faces, and iris from the Government of Mexico. Of these biometric modalities, only fingerprint and iris are matched against IDENT. A positive biometric match on an iris can trigger a manual fingerprint review from an examiner. Iris and fingerprints are used in the determination of identity when supplied by the submitting foreign partner. This PIA will be updated should any additional biometric modalities be matched against IDENT.

[11] *See supra* note 4.

[12] *See supra* note 7.

[13] *See supra* note 5.

[14] ARIES will establish a connection with UPAX to foster the existing information sharing processes. For example, currently transactions that are designated as BITMAP submissions by the Government of Mexico will be submitted to UPAX to be incorporated as part of BITMAP. Additionally, all acknowledgment responses from foreign partner submissions (currently Mexico) are sent to UPAX for identity analysis. This allows UPAX to retrieve identities from IDENT to analyze and review information associated with foreign partner submissions.

[15] *See supra* note 6.

[16] IXM is a method of communicating with IDENT/HART in Extensible Markup Language (XML) message format. The XML-based format is designed to perform specific operations in IDENT/HART Services for the IDENT/HART user or data provider and allows the IDENT/HART user or data provider to send or receive information to IDENT/HART.

[17] *See supra* note 8. System configurations that reflect the permissions of each HART authorized user as agreed to in ISAAs with OBIM or DHS and as described in DHS Component-specific privacy compliance documentation. Business rules can also be configured to block sharing of biometric data in response to a query.

information that passes through ARIES based on incoming submissions. The business rules identify users and uses for systems connected to the ARIES technology (e.g., DHS IDENT/HART, DoD Automated Biometric Identity System, CBP Automated Targeting System Framework UPAX, and DOJ FBI Next Generation Identification). Lastly, the ARIES infrastructure can validate the format of information, decrypt, re-encrypt, and run virus scans on all incoming submissions.

Administration Application

ARIES is designed to ensure maximum administrative capability with minimal development to perform basic tasks such as user onboarding, business rule configuration, audit logging of transactional information, automated report generation, and both functional and regression testing of system changes. The Office of Biometric Identity Management is developing Biometric Guidelines which will provide IDENT/HART users and data providers with basic expectations on accuracy and responsible use of identification and analysis activities within the system.

User Interface

ARIES maintains a user interface responsible for displaying identity request and response information as well as generating vital operational statistics (i.e., allowing users to view the number of submissions, errors, and responses that are exchanged through the system).

There are two concepts of "user" to ARIES. One is a user of the client application, and the other is a user of the infrastructure. While the Office of Biometric Identity Management maintains access to the ARIES client, Components can use the ARIES technology to properly route their submissions to designated locations within the federal government to process those transactions in accordance with their current policy and privacy documentation. The infrastructure enables the proper routing of foreign partner submissions to the designated repositories for searching or analytical facilitation in accordance with current business rules.

The part of the client that allows access to the information passing through ARIES is read only. The administration of the system will require additional access controls that are administered by OBIM. Components already get the data that is in ARIES through their own systems.

ARIES will generate a single web-based user interface with associated user roles and business rules to enable users to read information generated by their processed submissions. These submissions are based on previously agreed upon permissions. The Office of Biometric Identity Management controls the ARIES user interface which maintains username and login data access controls that restrict the functionality and data access based on the role of the authenticated user. The ARIES user interface will be accessible to OBIM users.

The user interface will maintain tools for the ingestion of bulk identity data from the foreign partner and the generation of analytical metrics, such as daily, weekly, and monthly reports and identity reports, using the data that has traversed the system. These metrics include operational statistics such as the number of submissions, the number of responses, response times, data subjects' nationalities, and the number of data subjects with derogatory information.

Bulk identity data may include information that was not originally collected by electronic means, such as digitally scanned ink fingerprint cards that were generated by the foreign partner prior to development of the foreign partner's electronic system. The user interface will also allow authorized users to add or remove derogatory information to and from a submitted identity based on the research and analysis conducted in real time.

Access Controls

The DHS Office of Biometric Identity Management will administer the Amazon Web Services cloud space for configuration management and development updates. The user base will include DHS, DOJ, DOS, and DoD agency representatives to facilitate biometric information sharing. OBIM controls the access rights including the ability to create a user profile granting access rights and limitations directly from the ARIES user interface.

ARIES Process

ARIES uses biometric and biographic information collected by foreign partners and provided to DHS through various bilateral biometric information sharing access agreements (ISAA) to authorize DHS bilateral biometric identity information exchange between the U.S. Government and designated foreign partners. ARIES will collect and sort identity data using an established transaction control number (TCN) in a list format for review by DHS, DOS, DOJ, and DoD users authorized to access ARIES. ARIES displays a list of identities submitted by foreign partners that can be sorted by various fields such as derogatory information,[18] country of submission, country of birth, and response status and completion metadata to allow the OBIM prioritize and review. Biometric response data collected by the individual repositories such as the

[18] Derogatory Information (DI) is information which potentially justifies unfavorable suitability, fitness, or security adjudication, and such information may prompt a request for additional investigation or clarification for resolution of an issue. *See* DHS Instruction 121-01-007-01 for Personnel Security, Suitability and Fitness Program (August 2016), on file with the DHS Privacy Office. HART users will have the ability to add or deactivate DI. Deactivating a particular DI demotes the DI. HART will not include that deactivated DI element in the response to the Authorized user. DI may include information submitted from the DoD, FBI, DOS, INTERPOL, international country partners, and DHS Components, specifically ICE and CBP.

DoD ABIS,[19] DOJ NGI,[20] OBIM IDENT/HART,[21] and CBP UPAX[22] will be available for the applicable DHS, DOS, DOJ, and DoD users.

ARIES will automatically validate the proper Organization/Unit/Subunit (OUS)[23] appended to the incoming submission to ensure that IDENT/HART is able to apply the proper data field, special protected classes,[24] encounter, and other filtering prior to responding to the foreign partner's request. ARIES will use pre-established IDENT/HART business rules to comply with all programmatic policies and privacy guidelines set forth in the documentation that governs the foreign partner connection. These guidelines include the proper application of an Organization/Unit/Subunit to IDENT/HART and the suppression of an NGI and/or ABIS data response to the foreign partner as applicable. Foreign partners that receive information that passes through ARIES will not have direct access to ARIES.

Security Protocols

ARIES uses secure Amazon Web Services in the Federal Risk and Authorization Management Program (FedRAMP)[25] certified cloud that ensures that security protocols have been applied to reduce the threat of unauthorized access to data. Amazon Web Services enables analytics, reporting, data brokering, business rules, configuration management, and access controls to be used for international information sharing. The ARIES technology holds all DHS technological security requirements to protect the personally identifiable information (PII) and all applicable DHS security protocols to ensure the proper encryption and security of the data traversing the platform.

ARIES uses the Trusted Internet Connection (TIC)[26] enabled through DHS OneNet for the routing of all information across DHS systems for the purpose of engaging established transaction

[19] *See supra* note 7.
[20] *See supra* note 6.
[21] *See supra* note 4.
[22] *See supra* note 5.
[23] IDENT/HART uses an Organization/Unit/Subunit (OUS) structure to identify the submitter/owners and requestors of encounters in IDENT. The OUS is used to provide a high-level descriptor of the Organization, agency, and mission utilizing the IDENT/HART database. It is further discussed in the HART Increment 1 Privacy Impact Assessment. *See supra* note 5.
[24] Certain classes of individuals who are filing for immigration benefits where additional confidentiality restrictions exist on the sharing of information. This includes Violence Against Women Act (VAWA), T cases, U cases, Asylum and Refugee Cases, Temporary Protected Status (TPS), Legalization and Special Agricultural Worker (SAW) cases, S cases, and the Witness Security Program. These individuals receive special confidentiality through statute, regulation, or DHS policy.
[25] The cloud service provider is required to adhere to the security and privacy controls set by the National Institute of Technology (NIST) Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing," and the DHS Chief Information Officer. *See* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.
[26] The purpose of the Trusted Internet Connections (TIC) initiative, as outlined in the Office of Management and Budget (OMB) Memorandum M-19-26: Update to the TIC Initiative, is to enhance network and perimeter security

security protocols and line encryption methodologies. ARIES will use a direct administration application to ensure real-time compliance of all DHS policy and privacy guidelines to administer the business rules and authorize and deauthorize access controls. OBIM's Identity Operations Division administers this application. ARIES uses Login.gov[27] for access control to the client application. Use of this service requires two-factor authentication as well as hardened password protection. Login.gov leverages the best security defined by NIST-800-63[28] Identity Assurance Level 1 and Authentication Assurance Level 2, and FedRAMP Moderate to secure validation and verification of identity prior to data access.

This PIA builds on the functionality of IDENT/HART and TRACS.[29] The HART Increment 1 PIA covers the core foundational infrastructure and baseline existing functionality in IDENT that ensures continuity of services without disruption to existing IDENT users. Due to the privacy risks associated with the collection, retention, use, and dissemination of biometrics, the DHS Privacy Office included recommendations throughout the "Privacy Impact Analysis" section of the HART Increment 1 PIA, which are also relevant to ARIES and the information sharing it facilitates. Those recommendations address Transparency, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, and Accountability and Auditing. Similarly, the TRACS PIA identifies unmitigated and partially mitigated risks regarding Transparency, Data Minimization, Use Limitation, Data Quality and Integrity, and Accountability and Auditing.

Section 1.0 Authorities and Other Requirements

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

The data in ARIES is collected, processed, and stored consistent with the applicable authorities of DHS and the agencies and mission partners that originally collected the data, as expressed in ISAAs with OBIM or agreements or arrangements with DHS. OBIM identifies each collection by data provider and implements the provider's authority to use, retain, and share the

across the federal government. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE AGENCY, DEFINITION FOR TRUSTED INTERNET CONNECTIONS, *available at* https://www.cisa.gov/trusted-internet-connections.

[27] Login.gov is an online identity platform that assists agencies in verifying their users are who they say they are from their own home. It offers the user online access to government programs. For more information, visit https://www.login.gov.

[28] *See* NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGY, IDENTITY GUIDELINES, *available at* https://pages.nist.gov/800-63-3/.

[29] See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE TECHNICAL RECONCILIATION ANALYSIS CLASSIFICATION SYSTEM (TRACS), DHS/OBIM/PIA-003 (2020), available at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

information according to the terms of the applicable ISAA, which may include a memorandum of agreement (MOA), memorandum of understanding (MOU), or other formal, data sharing policy. Many of these authorities are also described in the PIAs, System of Records Notices (SORN), or other documents for each of these agency programs.[30]

The statutory and other authorities pertaining to the establishment and mission of OBIM, including the operation and maintenance of IDENT/HART, include:

- Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106–215, codified at 8 U.S.C. § 1365a;
- Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, Div. C, 110 Stat. 3009-546 (Sept. 30, 1996);
- Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106–396, codified at 8 U.S.C. § 1379;
- Sections 403(c) and 414(b) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT); Pub. L. No. 107–56, codified at 8 U.S.C. § 1379, 8 U.S.C. § 1365a, 8 U.S.C. § 1365a note;
- Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107–173, codified at 8 U.S.C. §§ 1722, 1731;
- Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, codified at 8 U.S.C. § 1365b;
- Section 711(d) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, codified at 8 U.S.C. § 1187;
- Consolidated Appropriations Act of 2017, § 301 Pub. L. No. 115-31, 131 Stat. 135 (2017);
- Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013);
- 8 CFR § 214.1, U.S. Department of Homeland Security, Immigration Regulations, Nonimmigrant Classes, Requirements for Admission, extension and maintenance of status (January 1, 2012);
- 8 CFR § 208.6, U.S. Department of Homeland Security, Immigration Regulations, Procedures for Asylum and Withholding of Removal, Asylum and Withholding of Removal Status (January 1, 2012);

[30] *See* Appendix A – Privacy Compliance Documentation for additional information.

- 8 CFR § 235.1, U.S. Department of Homeland Security, Immigration Regulations, Inspection of Persons Applying for Admission, Scope of Examination (January 1, 2012);
- Homeland Security Presidential Directive/HSPD-11: Comprehensive Terrorist Related Procedures (August 27, 2004); and
- Homeland Security Presidential Directive/HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 5, 2008).

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

The information in ARIES is covered by the source system DHS, DHS Component, and partner SORNs, which govern the function and use of the biometrics records collected by each Component. DHS information in ARIES relies on the DHS/ALL-041 External Biometric Records (EBR) System of Records to govern the maintenance and use of biometrics and associated biographic information received from non-DHS entities.[31] The Enterprise Biometric Administrative Records (EBAR) SORN will cover administrative records maintained in HART.[32]

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

The Authority to Operate (ATO) for this system will be granted upon completion of this PIA and in accordance with other requirements of DHS Management Directive 4300A.

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

Each U.S. Government system with which ARIES interfaces retains information based on its own approved NARA retention schedule. The NARA approved records schedule requires OBIM to maintain IDENT/HART records in its custody for the various retention periods outlined in the Biometric with Limited Biographic Schedule (DAA-0563-2013-0001).[33] There is currently no records schedule for ARIES transactional data, so records will be treated as permanent until there is an approved NARA records schedule. OBIM is re-evaluating the current retention policy to determine variable retention periods for latent fingerprints, international records, and transaction

[31] *See* DHS/ALL-041 External Biometric Records (EBR), 83 FR 17829 (May 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[32] *See* DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR), 85 FR 14955 (March 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[33] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0563-2013-0001, U.S. DEPARTMENT OF HOMELAND SECURITY, BIOMETRIC WITH LIMITED BIOGRAPHICAL DATA (2013), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

records and will publish a PIA update that will address any changes to retention periods. NARA retention schedules and compliance are enabled by the organization that permanently retains the encounter identity data such as OBIM IDENT/HART, DOJ NGI, DoD ABIS, and CBP UPAX.

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

The ARIES technology is not responsible for collecting information covered by the PRA. All information stored in IDENT/HART is collected by IDENT/HART data providers and stored under the data provider agency's regulatory notices and authorities.

Section 2.0 Characterization of the Information

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

ARIES provides a user interface for biometric identity information exchange between the United States and applicable foreign partners. ARIES implements current DHS security standards, proper formatting of encounter submissions for the applicable U.S. Government systems, and message routing. Fingerprints, facial images, and associated biographic information collected by the foreign partner are sent by foreign partners through ARIES to IDENT/HART. Fingerprints are queried against IDENT/HART and IDENT/HART indicates whether a fingerprint match exists by automatically responding "match" or "no match" to the querying country. If there is a shareable fingerprint match, IDENT/HART uses its data access and security controls to filter out identity data that cannot be shared and send only permissible information back to the foreign partner. IDENT/HART's business rules dictate what information may be shared; ARIES itself does not determine what information is sharable and what is not, nor does it execute any biometric matching requirement.

Information supplied by IDENT/HART in accordance with its current policy/privacy/legal data access and security control requirements is supplied to ARIES to be translated into the proper messaging format and routed appropriately back to the requesting foreign partner. The process of data matching, storing, responding, and filtering applicable data sets from a DHS response to the foreign partner's response message occurs today in IDENT. ARIES provides available biometric (e.g., fingerprints, digital facial photograph) and biographic data (e.g., biographic encounter information, encounter metadata) from IDENT/HART to foreign partners consistent with law and policy, which may include: first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, facial photographs, current and former nationalities, passport data, numbers from other identity documents, U.S. immigration history,

descriptions of past enforcement actions, and encounter information (e.g., transaction-identifier data including the sending DHS organization; timestamp; reason collected, such as entry, credentialing application, or apprehension; and any available encounter information). IDENT may filter out, on an automated basis, information based on DHS policies, statutes, agreements, and previously established data sharing rules and IDENT's data sharing configuration rules.

ARIES displays biographic data in the user interface to designated U.S. Government personnel for the purpose of identity adjudication, threat coordination, reporting, and analytics. ARIES allows a user to see the identity data that was provided to the foreign partner along with the full IDENT identity for complete visibility into the information exchange with the foreign partner.

IDENT/HART

IDENT and HART are the central DHS-wide systems for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses.

Encounter information (e.g., facial images, iris scans, biographic information, and encounter metadata) are enrolled in the IDENT/HART database based on fingerprints and are maintained and searched for the purposes of reporting, analytics, and identity response enhancement consistent with the terms of the relevant ISAAs between DHS and the foreign partner. In accordance with the IDENT/HART IXM[34] format, OBIM applies information such as the Organization/Unit/Subunit, activity type, activity reason, and comment language to the encounter information. These measures support proper dissemination of encounter information back to authorized users in the event of a subsequent biometric match. The aforementioned specified fields annotate the origin of the encounter submitted by the foreign partner and enable the application of data business rules by IDENT/HART for the filtering of sensitive and/or non-sharable information in accordance with applicable law and policy.

If a fingerprint match is found, then OBIM currently shares the following biometric and biographic data according to law and policy: first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, facial images, current and former nationalities, passport data, numbers from other identity documents, immigration history, descriptions of past enforcement actions, and encounter information (e.g., transaction-identifier data including the sending organization; timestamp; reason collected, such as entry, credentialing application, or apprehension; and any available encounter information).

[34] *See supra* note 16.

In instances where the messaging format differs from that of IDENT/HART, ARIES will properly format the automated response from IDENT/HART and provide it back to the foreign partner in compliance with the ISAAs between the foreign partner and DHS and in accordance with existing U.S. law and DHS policies.

To use the full breadth of IDENT/HART data, an authorized ARIES user can execute an identity retrieval of the individual using an unfiltered Organization/Unit/Subunit to display all available identity data to adjudicate the prioritized identity. The identity retrieval provides all encounter information and derogatory information associated with the identity to provide OBIM adjudicators with as much information as possible to assess the risk level of the individual to the United States and/or the foreign partner.

Identity retrieval information from IDENT/HART displayed in ARIES includes: first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents, immigration history, descriptions of past enforcement actions, encounter information (e.g., transaction-identifier data including the sending organization; timestamp; reason sent, such as entry, credentialing application, or apprehension; and any available encounter information), comment language, derogatory information, and criminal history.

The information contained within the complete identity response is not automatically shared with the foreign partner but is used by OBIM analysts to make informed manual information sharing decisions based on national security risk to both the U.S. Government and the foreign partner. OBIM receives daily match results and forwards these results to the appropriate entity for awareness and action on their part. ARIES provides the pathway for foreign partners and U.S. Government personnel to share fingerprint-based information used in manual analysis.

As mentioned earlier, DOS does not have a fingerprint-based system; DOS data is exchanged through IDENT/HART.[35]

FBI NGI

The FBI NGI[36] system is a central repository for persons fingerprinted because of arrest, incarceration, or other authorized criminal justice and non-criminal justice purposes. When the business rules of the signed agreement between the FBI and the foreign partner and/or the agreement between DHS and the FBI allow, encounter information (fingerprints, face, iris,

[35] *See* STATE-26 Passport Records, 80 FR 15653 (March 24, 2016) *available at*https://www.federalregister.gov/documents/2015/03/24/2015-06691/privacy-act-system-of-records-passport-records-state-26; STATE-36, Security Records, 83 FR 28058 (Jun. 15, 2018) *available at* https://www.state.gov/wp-content/uploads/2019/05/Security-Records-STATE-36.pdf; and STATE-39 Visa Records, 83 FR 28062 (June 15, 2018), *available at* https://www.state.gov/wp-content/uploads/2019/05/Visa-Records-STATE-39.pdf.

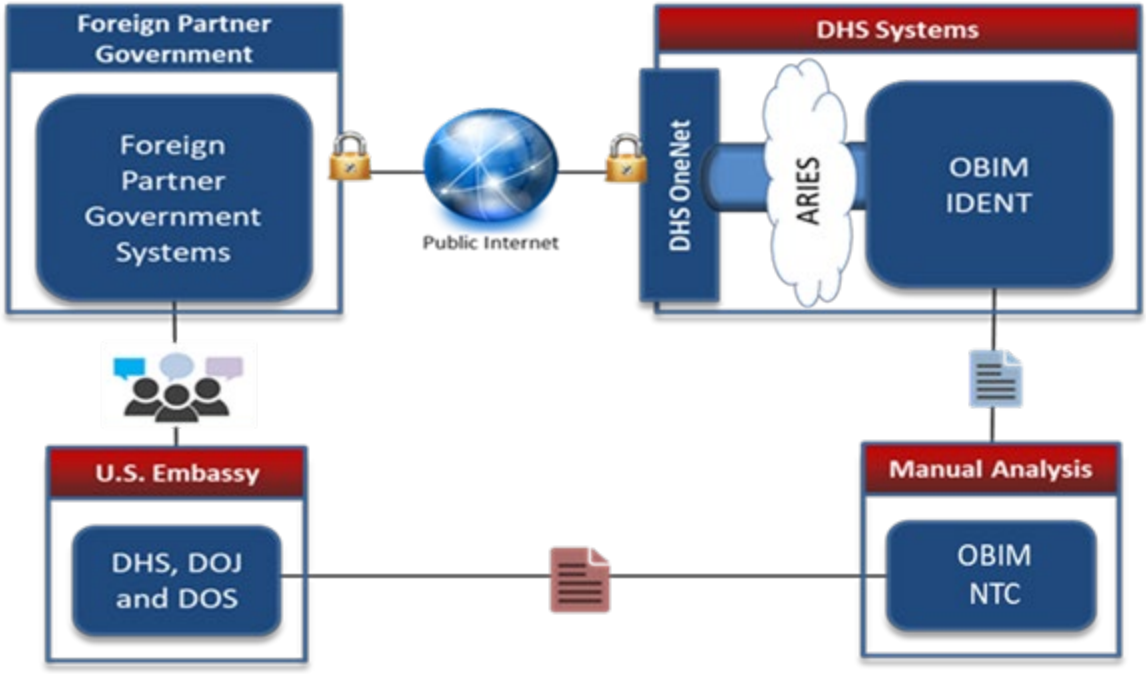
[36] *See* JUSTICE/FBI-009 Next Generation Identification (NGI) System, 81 FR 27284 (May 5, 2016), *available at* https://www.govinfo.gov/content/pkg/FR-2016-05-05/pdf/2016-10120.pdf.

biographic information, and encounter metadata) is searched and/or enrolled/stored in the NGI database for the purposes of reporting, analytics, and identity response enhancement.

DoD ABIS

DoD ABIS[37,38] is responsible for the storage, management, sharing, retrieval, and display of biometric data of U.S. and non U.S. neutral, known, and adversary individuals for timely identification for timely identification or identity verification. When the business rules of the signed agreement between DoD and the foreign partner and/or the agreement between DHS and DoD allow, encounter information (fingerprints, face, iris, biographic information, and encounter metadata) is searched and/or enrolled/stored in the ABIS database for the purposes of reporting, analytics, and identity response enhancement.

Foreign Partner Submission Process Flow



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

[37] *See* A0025-2 PMG (DFBA) DoD - Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/581425/a0025-2-pmg-dfba-DoD/.

[38] *See* A0025-2 SAIS DoD - Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569938/a0025-2-sais-DoD/.

ARIES does not directly collect information from individuals. ARIES receives information collected by federal, state, local, tribal, territorial, and foreign partners and submitted to DHS. Information received by the ARIES technology is filtered through the DHS OneNet TIC from a foreign partner submission encrypted and transmitted across the internet. After the application of established business rules, ARIES then receives response information from respective U.S. Government data repositories to display to OBIM as authorized by those agencies to support their mission purposes. Information sources include foreign partners participating in bilateral information exchange programs, IDENT/HART, DOJ NGI, DOS, and DoD ABIS.

Not all encounters will be shared, searched, or otherwise processed by all the aforementioned data sources. ARIES applies business rules, developed by OBIM and the data owners, to disseminate and compile data in accordance with the user authorities and policies.[39] ARIES maintains active connections with each foreign partner government system provider data source to ensure that data business rules can be applied quickly and effectively to increase or decrease information sharing to the respective data sources for the purposes of legal, privacy, and policy compliance. DHS requires the shared data to be consistent and permissible under the bilateral ISAA. DHS may designate additional information to share or not to share. In instances where this information may not be shared, OBIM personnel will temporarily retain information mentioned above for the purpose of identity analysis.

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

ARIES does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

ARIES ensures the proper formatting of the incoming foreign partner transaction, the submission of that transaction to the authorized data repository, the compilation of data source information for display, and the dissemination of the authorized response data back to the submitting foreign partner. ARIES flags incoming partner submissions that lack the proper fields to enable a biometric search of the applicable system.

[39] The HART Increment 1 PIA contains the following Privacy Office Recommendation: OBIM should establish a governance board made up of OBIM, DHS authorized users and providers, and DHS oversight offices (i.e., DHS Privacy Office, DHS Office of Civil Rights and Civil Liberties, Office of the General Counsel) to ensure that internal and external collection and dissemination of HART records is aligned with the data owner authorities and policies as set out in the business rules. The governance board should also review whether business rule configurations align with ISAAs with OBIM or agreements or arrangements with DHS that contemplate sharing from the HART system. *See supra* note 4.

ARIES will use the information contained within the foreign partner submission and the collective identity responses provided by the U.S. Government operational data sources to highlight possible discrepancies between the collective data sources. OBIM analysts then manually review the information displayed in the ARIES technology. These analysts can see the displayed information compiled from all authorized sources for a complete view of the biometrically validated identity data on file for the submitted identity. The analyst then manually provides and assessment back to the requester. DHS, DOS, DoD, and DOJ use the information transmitted through ARIES to support programmatic decisions.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A risk exists that a foreign partner will not inform DHS that data that the foreign partner provided was inaccurate.

Mitigation: This risk cannot be mitigated. Although OBIM has a dedicated team that continually monitors and reports on DHS sharing with other countries, it is possible that OBIM may not be able to identify inaccurate data provided by the partner country.

When a country becomes aware that material data it transmitted or received is inaccurate, unreliable, or subject to significant doubt, under the terms of the applicable ISAA, it is responsible for notifying the other country and taking all appropriate measures to safeguard against erroneous reliance on such data, which may include supplementation, deletion, or correction of the data.[40] Under the terms of the information sharing agreements, the parties have stated their intent to promptly notify and provide correct information—if available—to the other country if they believe the other country may be using or relying on inaccurate information exchanged under the information sharing arrangement. that country. Both the United States and its foreign counterparts intend, in accordance with their respective domestic laws, to provide persons who are the subject of information exchanged under the respective agreements with opportunities to request access to that information, to request correction of erroneous information, or to request to add a notation to indicate a correction request was made.

If ARIES flags inconsistencies in the data fields, OBIM will notify the respective data owner to review and correct the inaccurate information. ARIES supports the manual review of the biometrically matched identity information for rectification and deconfliction.

Privacy Risk: There is a risk that the quality and integrity of information collected through ARIES and maintained in IDENT/HART may be insufficient to serve its purpose of biometric and

[40] The HART Increment 1 PIA contains the following Privacy Office Recommendation: OBIM should establish a baseline quality for enrollment of all biometric modalities and provide guidance as to reliability of the modalities according to the age of the subject at the time of collection. *See supra* note 4.

biographic verification and matching, thus potentially causing false positive or false negative identification.

Mitigation: This risk is partially mitigated. The risk of false positive or false negative identification applies to IDENT/HART and the other systems which are queried during the process of facilitating an international biometric information sharing program and not associated with ARIES, the technology that is facilitating the exchange of data. IDENT/HART mitigates this risk by requiring fingerprints, which are unique identifiers, and basic biographic information, to establish an identity in IDENT/HART. The OBIM Biometric Support Center offers manual fingerprint comparisons of prints provided through ARIES when it is unclear whether they match a print in IDENT/HART. Additionally, IDENT/HART performs certain quality checks (e.g., determining the quality of a captured fingerprint and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness.

Privacy Risk: There is a risk that retaining the fingerprint, face, or iris biometric for juveniles may result in false positive or false negative matches due to factors including growth and image quality.

Mitigation: This risk is not mitigated.[41] This data quality issue applies to the program that enables the biometric data exchange and not the technology that is facilitating it. OBIM is currently retaining juvenile biometrics received from data providers in accordance with the memorandum titled "DHS Biometrics Expansion for Improved Identification and Encounter Management," signed by Secretary Kelly in May 2017.[42] This memorandum augments existing DHS policy to use biometric identification across all screening missions and to collect multimodal biometrics at the time of application or encounter, beyond the 14 and 79 years age range, when and where it is technically and operationally feasible. OBIM is in the process of isolating all juvenile biometrics in a separate gallery to minimize any impacts to matching accuracy.

To ensure accurate matches for fingerprints, IDENT/HART returns a limited number of possible matches to trained and experienced fingerprint examiners in its Biometric Support Center.

---

[41] The HART Increment 1 PIA contains the following Privacy Office Recommendation: OBIM should coordinate with applicable HART users and technical teams to analyze and determine if a separate O/U/S for minors should be maintained and how to effectively include validation checks with the data owners to ensure appropriate access controls. An additional DHS Privacy Office Recommendation is as follows: As a service provider, OBIM should provide expert guidance to data owners regarding the length of time a particular biometric remains valid for comparison. For example, a facial image of a young child may not provide a good match for the same individual when he or she is an adult. OBIM may be able to provide perspective to data owners on how to properly propose retention schedules. As previously stated, another DHS Privacy Office Recommendation includes: OBIM should establish a baseline quality for enrollment of all biometric modalities and provide guidance as to reliability of the modalities according to the age of the subject at the time of collection. *See supra* note 4.

[42] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, BIOMETRICS EXPANSION FOR IMPROVED IDENTIFICATION AND ENCOUNTER MANAGEMENT MEMORANDUM (May 24, 2017), *available at* https://www.dhs.gov/publication/dhs-biometrics-expansion.

Biometric Support Center fingerprint examiners make a final determination on whether the submitted print matches any of the fingerprints currently retained in IDENT/HART. If Biometric Support Center examiners confirm that there is a match in IDENT/HART, the submitting agency can request additional information on the individual.

Additionally, OBIM is following and monitoring industry best practices, including research from the Center for Identification Technology Research (CITeR),[43] as it continues to conduct studies and evaluate biometric modalities and matching for children under 14.

Privacy Risk: There is a privacy risk that data quality will not be maintained since IDENT/HART users can manually apply derogatory and disposition information.

Mitigation: This risk is not mitigated. OBIM cannot ensure accuracy in ARIES since the information is not automatically pulled from the source system. OBIM coordinates with users to determine what derogatory information they are authorized to share. Additionally, OBIM will train IDENT/HART users on how to use IDENT/HART's derogatory services in accordance with the user's source system mission and business rules.[44]

Privacy Risk: There is a risk of collecting and sharing more information through ARIES than is required for the purposes of the programs it supports, because its direct connection—IDENT/HART—cannot filter by biometric modality and collects biographic data that details the subject's encounters, which are not strictly necessary for all program purposes.

Mitigation: This risk is partially mitigated. OBIM's foreign and U.S. Government partners share information with OBIM via ARIES based on various ISAAs. The ISAAs generally state what information the partners should exchange. Through ARIES, IDENT/HART shares different types of responses with different users based on a specifically articulated purpose as specified in the applicable ISAA. For certain data providers, the full encounter history of an individual's biometric interactions with the Department is required to meet the mission of the agency. For example, a data provider may determine whether non-derogatory information should be shared with IDENT/HART authorized users based on agreements or policy. OBIM configures IDENT/HART with business rules to withhold such data from the response. The business rules

[43] *See* information on Center for Identification Technology Research (CITeR), *available at* https://citer.clarkson.edu/affiliates/.

[44] *See supra* note 4. The HART Increment 1 PIA contains the following Privacy Office Recommendation: When drafting the OBIM Biometric Guidelines, OBIM should consider content that will assist data users and data providers when determining accuracy, the parameters for providing candidate lists, a description of Biometric Support Center examiner services, the requirements and retention period for probes (e.g., latent prints and facial images), any prohibitions on intentional alteration of an original biometric, any required training for HART system use, responsibilities for adherence to the applicable records retention schedule, and OBIM's audit schedule for HART. The OBIM Biometrics Guidelines should also describe the tuning and business rules process as it applies to all biometric modalities. An additional DHS Privacy Office Recommendation is as follows: The DHS Privacy Office recommends OBIM develop additional privacy-specific training and material based on a HART user's mission need and job function.

can also be configured to block sharing of biometric data in response to a query. IDENT/HART responses through ARIES are appropriately scoped to the purpose of each authorized user, as memorialized in an ISAA with DHS and applicable DHS Component privacy compliance documentation.

Privacy Risk: There is a risk that OBIM analysts who use the data provided through ARIES will rely on DHS source data that is incomplete or out of date.

Mitigation: This risk is partially mitigated. OBIM cannot ensure the accuracy of data provided through ARIES since OBIM does not collect the data. The original data owner, whether an organization external or internal to DHS, is responsible for ensuring the accuracy, completeness, and quality of the data submitted to OBIM through ARIES. OBIM coordinates with users to implement sharing based on the legal and policy requirements of the parties. Additionally, in coordination with U.S. Government data owners, OBIM will train IDENT/HART users on how to use IDENT/HART's services in accordance with the user's source system mission and business rules to deconflict.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The ARIES technology formats and routes transactional foreign partner queries to authorized data repositories and queries from the United States to foreign partner data repositories for programs that rely on fingerprint-based data exchange. These data exchange programs operate pursuant to separate legal authorities and have separate policy compliance documentation and ISAAs. The information that is returned to the foreign partner through ARIES is governed by data business rules that are consistent with the IDENT/HART business owners' PIAs and SORNs (see Appendix A). The repository being searched filters prohibited data such as special protected classes identities, protected encounters, specific derogatory information, and/or specified data fields in accordance with the established documentation. ARIES maintains the ability to search a data source such as DoD ABIS or DOJ NGI and suppress the responses provided by those repositories from being disseminated to the requesting foreign partner.

Full and unfiltered identity information retrieved from any data source queried through ARIES will be temporarily retained and displayed within an identity adjudication client for review by OBIM and NTC analysts for the purposes of manual information sharing with a foreign partner when permissible. OBIM will also provide identity analysis, trend analysis, and/or internal interagency coordination for required action. IDENT/HART automatically suppresses information that is not sharable under current DHS policy with a foreign partner. This includes certain information contained within the unfiltered replies to the requesting foreign partner. The information collected because of the additional retrieval of unfiltered identity information is only

for the relevant purpose of the OBIM internal manual adjudication processes via TRACS.[45] The ARIES technology automatically facilitates data exchanges consistent with the business rules OBIM programs into IDENT/HART.

Information displayed in the identity adjudication client application includes: first and last names, former names, other names, aliases, alternative spelling of names, gender, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents, immigration history, descriptions of past enforcement actions, and encounter information (e.g., transaction-identifier data including the sending organization; timestamp; reason sent, such as entry, credentialing application, or apprehension; and any available encounter information), comment language, derogatory information, criminal history, and associated biometric information. OBIM analysts use this information only for the expressed purposes of identity adjudication, reporting, analysis, and operational coordination.

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

No. ARIES allows OBIM users to generate reports that include operational statistics on increased transaction volumes, identity counts by age, gender, nationality, or encountered country, and geospatial location analysis. However, ARIES is not used to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

ARIES will be used by OBIM to facilitate the routing, formatting, and analysis of identity information. ARIES ensures that information is initially received by IDENT/HART, which passes the information to NGI and ABIS from a foreign partner. Individual Components such as U.S. Citizenship and Immigration Services (USCIS), ICE, and other DHS Components will access ARIES based on mission need. ARIES routes information in accordance with business rules written in international information sharing agreements, to DoD and DOJ. Information collected by foreign partners passes through ARIES for business rule application, formatting, routing, and to facilitate analysis within IDENT/HART.

OBIM will disseminate analytical products facilitated by ARIES to DHS Components, leadership, and external agencies, as permissible, on a need-to-know basis for the purpose of

[45] *See supra* note 29.

providing identity data and analytics. OBIM regulates access to ARIES based on the authorities of the requesting entities (see Appendix A).

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that ARIES users may use information for purposes inconsistent with the purpose of the original collection.

Mitigation: This risk is partially mitigated. ARIES is a tool, and its use does not create new policies for access to or handling of personal information. For DHS, ISAAs between OBIM and data providers and OBIM and data users will ensure the business rules implement compatibility of collection and use as discussed in the HART PIA.[46] IDENT/HART records audit trails of changes made to service request processing priorities and changes made to system operating parameters and thresholds. More specifically, IDENT/HART tracks and logs changes made to business processing rules, Service Level Agreements (SLA), accounting of disclosures of PII, all outgoing transaction data (excluding biometric images) sent as part of an outgoing identity message, authorized and unauthorized actions, deletions, modifications, errors, exceptions, and actions performed by users accessing the data. Quality assurance audits will be available to all IDENT/HART authorized users and oversight offices.

Individuals requiring access to the system will be OBIM employees or cleared contract staff, and as such are subject to section DHS 4300A Handbook Attachment G—Rules and Behavior, which establishes the DHS policy regarding the recognition, identification, and safeguarding of Sensitive Security Information.

Section 4.0 Notice

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

This PIA provides general notice that an individuals' personal information may be temporarily retained by ARIES. The IDENT PIA,[47] HART PIA,[48] NGI PIA,[49] NGI SORN,[50] ABIS SORN,[51] EBR SORN,[52] and EBAR SORN[53] provide further notice that DHS and other U.S.

[46] *See supra* note 4.
[47] *See supra* note 4.
[48] *See supra* note 4.
[49] *See supra* note 6.
[50] *See* JUSTICE/FBI-009 Next Generation Identification (NGI) System, 84 FR 54182 (October 09, 2019), *available at* https://www.federalregister.gov/documents/2019/10/09/2019-21585/privacy-act-of-1974-system-of-records.
[51] *See* Appendix A – Privacy Compliance Documentation for additional information.
[52] *See supra* note 31.
[53] *See supra* note 32.

Government agencies may retain an individual's personal information. Notice is also provided through the publication of PIAs and SORNs on the underlying systems of original collection and the information shared from those systems. If required by law or policy, DHS Components, as well as external partners that submit information to HART and other DHS systems, provide notice to the individual at the point of collection related to storage and retention of information, including whether it is retained initially in IDENT or currently in IDENT/HART.

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

ARIES operates as a data exchange. Individuals should consult source system DHS programs (available in Appendix A) for specifics on opportunities to opt-out and consent. Information received from outside of DHS may or may not offer users the opportunity to opt-out or consent.

The ability of an individual to decline the collection by the foreign partner is the sole responsibility of the foreign partner to apply in accordance with their laws and policies.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that information collected directly from them is analyzed by the ARIES infrastructure through information-based searches of data providers' databases.

Mitigation: This risk is partially mitigated. Publication of this PIA provides notice of ARIES and the searching that occurs with data providers' databases. However, because OBIM is not the original collector of the information, it cannot sufficiently provide notice to all individuals. Notice of the use of information is provided by publishing this PIA and all corresponding PIAs[54] associated with the international biometric information sharing programs that are facilitated by the ARIES technology. The collecting foreign partner agency is responsible for providing notice at point of collection that the information may be shared with other U.S. federal, state, local, and foreign government agencies, and authorized organizations following approved routine uses described in the associated published SORNs. For information collected by foreign government agencies and submitted to ARIES for the application of business rules and transmission to the applicable data repository, this risk is mitigated to differing degrees depending on what notification mechanisms may be used by those original collectors.

Section 5.0 Data Retention by the Project

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

[54] *See* Appendix A – Privacy Compliance Documentation for additional information.

ARIES retrieves information through biometric or biographic searches for the purpose of identity analysis and transactional display. ARIES will maintain a database of all request and response data, for a period of 60 calendar days after the receipt of all applicable database searches. Information is collected and retained for a period of 60 days to ensure the proper time to execute the identity information adjudication and to ensure that data is available for troubleshooting system issues in the event of transactional errors, queuing issues, or network outages. When the data reaches the 60-day cut-off period, ARIES will automatically and permanently delete the request and response PII, maintaining only basic transactional metadata such as date stamps, timestamps, encounter and transaction identifiers, and applicable references for audit logging capabilities. The aforementioned information will be used to ensure that a complete log of request and response transactions is maintained for the purposes of technological and systematic auditing requirements.

IDENT/HART maintains records for a variable period in accordance with National Archives and Records Administration (NARA)-approved records schedules.[55] OBIM is currently developing the transactional record systems retention schedule. Once complete OBIM will submit it to NARA for approval.

U.S. Government and international partners may retain information received via ARIES, consistent with their own policies, retention schedules, and ISAAs. OBIM currently keeps international records for 75 years. DHS is re-evaluating the current retention policy to determine whether a new retention period or combination of retention periods is appropriate. DHS will publish a PIA update for any change in the retention period.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that ARIES may duplicate PII associated with foreign partner and U.S. Government identity data.

Mitigation: This risk is partially mitigated. Although ARIES may duplicate PII associated with foreign partner and U.S. Government identity data, this PII is automatically and permanently deleted after 60 days. Information is retrieved and maintained for a period of 60 days to ensure the proper time to execute the identity information adjudication and to ensure that data is available for troubleshooting system issues in the event of transactional errors, queuing issues, or network outages. Therefore, if data is duplicated, it will only be maintained for a short period of time.

Privacy Risk: There is a risk that PII will be retained longer than is necessary.

Mitigation: This privacy risk is mitigated. ARIES will maintain a database of all request and response data, to include PII, for a period of 60 calendar days after the receipt of all applicable database searches for audit logging capabilities. Information is collected and retained for a period of 60 days to ensure the proper time to execute the identity information adjudication and to ensure

[55] *See supra* note 4.

that data is available for troubleshooting system issues in the event of transactional errors, queuing issues, or network outages. When the data reaches the 60-day mark, ARIES will automatically and permanently delete the request and response data, maintaining only basic transactional metadata such as date stamps, timestamps, encounter and transaction identifiers, and applicable references within ARIES.

Section 6.0 Information Sharing

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

OBIM shares analytical products, reports, data analysis, statistics, and associated information based on data that passes through ARIES with permitted federal, state, local, tribal, territorial, foreign, and international agencies for national security, law enforcement, criminal justice, immigration and border management, and intelligence purposes. Reports will be shared only with those who have the need to know and per existing IDENT/HART business rules.

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

ARIES will be used to share information with external entities as mentioned by the EBR SORN[56] consistent with Routine Uses J and K.

- Routine Use J covers sharing with federal, state, or local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order (E.O.), or other applicable national security directive.
- Routine Use K covers sharing of information with federal and foreign government intelligence or counterterrorism agencies or Components when DHS reasonably believes a threat or potential threat exists to national or international security for which the information may be useful in countering the threat or potential threat, or when disclosure supports the conduct of national intelligence and security investigations or assists in anti-terrorism efforts.

Additional SORN coverage outlining the applicable sharing is provided by the DHS-wide Enterprise Biometric Administrative Records SORN,[57] which allows the maintenance of DHS-

[56] *See supra* note 31.
[57] *See supra* note 32.

generated transactional information such as biometric indicator data, and additional DHS and Components SORNs.

6.3 Does the project place limitations on re-dissemination?

External data owners sign ISAAs that govern the sharing of data that passes through ARIES. ISAAs may include MOAs, MOUs, Implementing Agreements, or other formalized letters describing the purpose, use, and scope of sharing. Those ISAAs include limitations and restrictions on re-dissemination and third-party sharing. These limitations will be discussed in full in the user agreements associated with the international biometric information sharing programs that use the ARIES technology.

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

IDENT/HART retains an accounting of records disclosed outside of the Department for the purpose of international data sharing. The disclosures include records that are hardcopy or electronic and that record the date, nature, and purpose of each dissemination and disclosure, along with the name and address of the individual or agency to which the disclosure is made. This list of disclosures is retained as part of the accounting requirements for IDENT/HART to be able to recreate the information to demonstrate compliance. ARIES maintains a transactional data log that can allow visibility into information received by a foreign partner and the exchange process.

Both ARIES and IDENT/HART maintain an audit record in the database for each system message sent. Audit logs are maintained by both the IDENT/HART and ARIES programs. Access to audit logs is limited strictly to core OBIM personnel. The audit log data is backed up regularly as part of the overall ARIES and IDENT/HART database backup and archiving process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Because of the sensitivity of certain classes of individuals' data collected by DHS Components, there is a potential risk that ARIES may share sensitive data with groups not authorized to receive the data.

Mitigation: This privacy risk is mitigated. IDENT/HART contains information provided by USCIS on millions of applicants and petitioners seeking immigration benefits. Some of the individuals who have applied for and/or received immigration benefits belong to classes of individuals, referred to as special protected classes, because their information is subject to heightened confidentiality provisions by statute, regulation, or policy. These confidentiality protections generally prohibit or otherwise limit the disclosure or use of any information about

applicants for, and beneficiaries of, certain immigration benefits, including those applied for under 8 U.S.C. § 1367 and other provisions.[58]

IDENT/HART maintains filtering capabilities to ensure that data is shared only with data provider-approved agencies for approved purposes. IDENT/HART filters information by encounter, derogatory information, and specific data fields when it is provided to a foreign partner in compliance with applicable laws and policies. IDENT/HART applies an Organization/Unit/Subunit filter prior to data passing through ARIES. The Organization/Unit/Subunit filters response data according to current policy, privacy, and legal requirements. IDENT/HART passes a response message through ARIES; this message continues as the official response back to the foreign partner. ARIES. enables the reformatting of the message into the native language of the foreign partner; however, the response message maintains the data filtering rules applied by IDENT/HART as demanded by current information sharing authorities.[59]

Privacy Risk: There is a risk that ARIES may share information about individuals inconsistent with the outlined uses defined in the ISAA between the United States and the foreign partner.

Mitigation: This privacy risk is partially mitigated. DHS's enterprise biometric system, IDENT/HART, does not supply caveats in query responses. Foreign partners' audit and redress provisions, however, may be used to detect wrongfully shared information and provide redress. DHS PIAs related to sharing with foreign partners lend additional transparency to those external partners' provisions. Additionally, OBIM will audit information sharing in HART to ensure consistency with the ISAAs. ARIES allows for transactional audit logging. Both the U.S. Government and the foreign partner may agree to consult one another regularly on the implementation of their arrangements.

ARIES or the respective data repository can stop or reduce the information dissemination using administrative configurations. Any determined misuse may result in a termination of the applicable ISAA.

ARIES maintains a transactional metadata log to ensure proper tracking of information sharing and auditing compliance. Each agency supplying data is entitled to an accounting of what has been done with the data it supplied and the results obtained from that data.

IDENT/HART data providers and users have mission-based access limitations. OBIM implements access control within IDENT/HART through filtering capabilities, implemented through code, that can remove access to information at the organizational, encounter, and

[58] *See supra* note 24.
[59] The HART Increment 1 PIA contains the following Privacy Office Recommendation: The DHS Privacy Office recommends that HART implement caveats on data shared with foreign partners to ensure that they are aware of any restrictions that apply regarding use of the data. *See supra* note 4.

identity/person level based on purpose or activity type. Filtering can also be conducted based on derogatory information. OBIM encodes these data filtering authorizations through business rules, which are the system configurations that reflect the permissions of each IDENT/HART authorized user as agreed to in agreements with OBIM or DHS and as described in DHS Component-specific privacy compliance documentation. OBIM continuously conducts quality assurance monitoring and generates monthly, quarterly, and annual reports on its sharing with each partner country. If data is found to have been inappropriately shared, then DHS will take appropriate remedial actions.

Privacy Risk: A privacy risk remains that data will be shared more broadly than permitted.

Mitigation: This risk is partially mitigated. ARIES uses the information provided by respective data sources for dissemination to the foreign partner in an automated fashion. The IDENT/HART data owners must provide business rules prior to using the ARIES data exchange to ensure proper adherence to policy, privacy, and legal requirements when providing data to a foreign partner. HART places limitations on third-party sharing by limiting the amount of data shared based on specific circumstances described in information sharing access agreements.

Foreign partners are obligated under the respective bilateral information sharing arrangements to maintain a log of all data transmitted and received. OBIM continually monitors quality assurance and generates monthly, quarterly, and annual reports for each participating agency. If data is found to have been inappropriately shared, DHS will take appropriate action.

Privacy Risk: There is a risk that a third party will intercept the transmission of data between DHS and a foreign partner through ARIES.

Mitigation: This risk is partially mitigated. ARIES meets the current DHS standards for data encryption to protect sensitive PII. ARIES uses high security encryption protocols to facilitate biometric query and response capabilities. ARIES requires the use of Transport Layer Security[60] (TLS) on incoming foreign partner submissions and response messaging as it traverses the public internet to ensure proper encryption of high value data traffic. ARIES uses the DHS OneNet Trusted Internet Connection as a standard for the transmission and proper topological routing of its transactions from foreign partners and between technical infrastructures within DHS. The DHS OneNet Trusted Internet Connection is responsible for the optimization and standardization of the security of individual external network connections currently in use by federal agencies, including connections to the internet. This requirement increases the overall security of the program and enables standardized security protocols, already in place and approved by DHS, to ensure an additional layer of safety between the ARIES concept and the foreign partner.

Privacy Risk: There is a risk that a partner country may share DHS-provided data,

[60] Transport Layer Security is a security protocol designed to facilitate privacy and data security for communications over the Internet.

transmitted through ARIES, with a third party without first obtaining consent.

Mitigation: This risk cannot be mitigated. Although the cooperative information sharing arrangements permit the supplying country to inquire how its data was used and the result obtained, this request may not always be fulfilled; and even if this request were fulfilled, any remedial actions would be forward-looking and would not remedy or mitigate the unauthorized sharing that would have already occurred. Any misuse discovered may result in a termination of the applicable ISAA. ARIES maintains the ability to add an additional layer of security and data dissemination control to ensure rapid compliance in the event of a determination of noncompliance by the foreign partner.

Privacy Risk: There is a risk that sensitive data will be inadvertently shared with the querying country through ARIES.

Mitigation: This risk is partially mitigated. While the automatic and manual filtering processes are methodically performed, sensitive data may be inadvertently shared using ARIES with a partner country. For instance, an individual's special protected classes status may not have been known at the time of the sharing, or the individual's legal status may have changed after the information was shared with a partner country. DHS is obligated under the applicable data sharing arrangements to maintain a log of all data transmitted and received, which is transmitted to DHS personnel daily, to ensure such sharing is performed appropriately. Reports are generated, reviewed, and as applicable, distributed to ICE, USCIS, and the DHS Office of Strategy, Policy, and Plans. OBIM applies an identity flag to the entire identity for certain special protected classes, preventing all encounters for that individual from being returned to requestors prohibited from receiving that information. Certain responses may be filtered based on DHS policy and statutes. Per 8 U.S.C. § 1367 "anyone who willfully uses, publishes, or permits information to be disclosed in violation of this section or who knowingly makes a false certification under section 239(e) of the Immigration and Nationality Act shall be subject to appropriate disciplinary action and subject to a civil money penalty of not more than $5,000 for each such violation." In addition, PII that is protected by 8 CFR 208.6 will only be exchanged pursuant to applicable Secretarial Waivers. If information is found to have been inappropriately shared, DHS will take remedial action, such as increased training.

ARIES is a technical data exchange for information maintained in IDENT/HART. The HART Increment 1 PIA[61] describes additional source system information sharing risks.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their

[61] *See supra* note 4.

information?

U.S. citizens, lawful permanent residents, and covered individuals who have covered records under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. All individuals, regardless of citizenship, may obtain access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Requesters may indicate the modality for the basis of the search. Individuals may submit a request to Chief Privacy Officer/Chief Freedom of Information Act Officer, Privacy Office, Mail Stop 0655, U.S. Department of Homeland Security, 2707 Martin Luther King, Jr. Avenue S.E., Washington, DC 20528-0655.

Requests for information are evaluated to ensure that any release of information is lawful and does not disclose information that would cause a clearly unwarranted invasion of personal privacy or that would disclose techniques and/or procedures for law enforcement investigations or prosecutions.

Individuals can also request access to their records by contacting the agency that maintains the encounter record in such systems as DHS IDENT/HART, DOJ NGI, and DoD ABIS. Requests for information are evaluated to ensure that any release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

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

Individuals are advised of the procedures for correcting their information through the respective programmatic PIAs ARIES supports. ARIES provides message reformatting and routing and facilitates manual identity adjudication and reporting for U.S. Government agencies. ARIES itself does not generate encounter records but is a utility for the proper dissemination and analysis of data being provided by a foreign partner when compared to existing data collected by numerous programs that connect to IDENT/HART, NGI, and ABIS.

U.S. citizens and lawful permanent residents, as well as other covered persons with records covered by the JRA, may seek to amend inaccurate records by filing a Privacy Act amendment request under the Privacy Act. Those individuals covered under by the JRA or Privacy Act may direct all requests to contest or amend information to OBIM Privacy, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, DC 20598-0675. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment.

If an individual is dissatisfied with the response to his or her redress inquiry, then he or she can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at Chief Privacy Officer/Chief Freedom of Information Act Officer, Privacy Office, Mail Stop 0655, U.S. Department of Homeland Security, 2707 Martin Luther King, Jr. Avenue S.E., Washington, DC 20528-0655; or by fax: 1-202-343-4010; or online at https://www.dhs.gov/freedom-information-act-foia. As with access, amendments may be limited pursuant to applicable Privacy Act exemptions asserted by the U.S. Department of Homeland Security.

Additionally, travelers who wish to file for redress can complete an online application through the DHS Traveler Redress Inquiry Program (DHS TRIP)[62] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). For more information about the types of services DHS TRIP can provide, please visit https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, the individual will receive notification of receipt from DHS TRIP. DHS TRIP will review the redress form and will determine which component/agency will be able to respond most effectively to the submission. When a redress request is related to records maintained in IDENT/HART, DHS TRIP will coordinate with OBIM. OBIM will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request.

DOJ NGI redress procedures are annotated within the FOIA requirements in their respective privacy documentation at https://www.fbi.gov/services/information-management/foipa.

For the Department of Defense, all FOIA requests must be in writing: (letter, email/web form, or fax). The request should be labeled, "Freedom of Information Act Request," preferably within the request letter and on the envelope/subject line/cover page and address the request to the DoD Component(s) likely to have the information sought. If it is unclear which Component is likely to maintain the information requested, individuals may check the list of Requester Service Centers (RSC) which are divided into: Military Services, Combatant Commands, and Defense Agencies for the contact information for each RSC, or write to: Defense Freedom of Information Division, 1155 Defense Pentagon, Washington, DC 20301-1155.

Additional FOIA request requirements are annotated on the DoD Open Government web page at https://open.defense.gov/Transparency/FOIA/FOIA-Handbook/.

[62] See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002, available at https://www.dhs.gov/publication/dhs-traveler-redress-inquiry-program-trip.

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

Individuals are advised of the procedures for correcting their information through information available at the respective record repositories used by ARIES for the purposes of data analysis and identity adjudication. Each agency retaining data that is used for the analytical processes executed by the ARIES infrastructure is responsible for notification to individuals about the procedures required to correct or retrieve their personal information held by the agency.

Individuals are also advised of the procedures for correcting their information by contacting OBIM Privacy, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, DC 20598-0675. The redress procedures for travelers are established and operated by DHS through DHS TRIP, which can be accessed at www.dhs.gov/trip.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals, particularly non-U.S. persons, may not understand how to correct incorrect information about themselves in DHS IDENT or other sources in ARIES used for data analysis.

Mitigation: This risk is mitigated. DHS TRIP provides a redress process through a website that facilitates the submission and processing of redress requests. Any individual can request access to or correction of their PII regardless of their nationality or country of residence. This process has been described in the DHS TRIP PIA and information is available in multiple places on DHS's public website. Redress requests that come to TRIP where a traveler encountered difficulties at the port of entry due to information in IDENT/HART or transmitted through ARIES that needs to be modified or updated, are assigned via TRIP to OBIM. The OBIM redress team along with OBIM System Business Operations, after review, then makes appropriate corrections to the IDENT/HART record if warranted and makes that notation in TRIP.

Alternatively, any person may submit a request to have a record corrected by contacting OBIM Privacy, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, DC 20598-0675.

Other external data sources such as DoD ABIS and DOJ NGI also enable non-U.S. persons with the ability to correct encounter information through their standard redress process outlined on their FOIA web pages and through a manual written request procedure.

Section 8.0 Auditing and Accountability

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

ARIES is compliant with the requirements of DHS information technology security policy, particularly the *DHS Information Technology (IT) Security Program Handbook for Sensitive Systems* (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. ARIES is periodically evaluated by OBIM and DHS security offices to ensure that it complies with these security requirements.

ARIES provides audit trail capabilities to monitor, log, and analyze system transactions, as well as actions and system accesses of authorized ARIES users.

As ARIES contains data from a variety of sources, collected for a variety of the purposes, it is necessary to institute controls so that only those individuals with a need to know may access that data. ARIES has role-based access controls for the infrastructure and user interface, which limit individual access to the appropriate discrete data collections. Misuse of the data in ARIES is mitigated by requiring that ARIES users conform to appropriate security and privacy policies, follow established rules of behavior, and train adequately regarding the security of the system. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity. External connections must be documented and approved with both parties' signatures in an interconnection security agreement, which outlines controls in place to protect the confidentiality, integrity, and availability of the information shared or processed.

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

DHS provides comprehensive privacy training that all DHS personnel are required to complete within the first 30 days of their assigned entry on duty. This follows the high-level overview privacy training provided by DHS as part of new-employee orientation. Users of the ARIES system, and all employees and contractors supporting its systems, have limited access based on their roles and need to know, and they are trained in the handling of personal information and PII for mission- and non-mission-related data (e.g., human capital and employment data). Training on specific systems will be conducted as appropriate. All DHS system users must complete annual privacy refresher training to retain system access to related data.

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

ARIES access is provided on a case-by-case basis depending on an individual's role-based accounts, in which access to the information contained within ARIES is required for the

completion of international data sharing tasks and procedures. ARIES will be operated by OBIM. OBIM has documented standard operating procedures to determine which users may access the ARIES data. Individuals with system access must hold a U.S. Government security clearance, must have a need to know the information based on their job responsibilities, and must participate in security and privacy training.

Some contractors may have access to ARIES data. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate nondisclosure and use limitations, in addition to requirements enumerated in Section 8.1 of this document. OBIM ensures that all employees and contractors supporting its systems have limited access based on their roles and that they are trained in the handling of PII.

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

DHS policy requires that ISAAs, including MOUs, MOAs, and Implementing Agreements, are reviewed and approved by DHS oversight offices, including the DHS Privacy Office, as well as the relevant Component Privacy and Security Offices and Component System Owner.[63] DHS Component Privacy Offices, including OBIM Privacy, are required to review technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts, and advise DHS leadership and DHS Components on implementing corresponding privacy protections.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There remains a risk that a foreign partner agency may not report a privacy incident to DHS, including unauthorized access or disclosure of PII.

Mitigation: This risk is partially mitigated. As previously discussed, foreign partner government agencies are required to keep a log of data sent and received in accordance with the documentation or agreement that governs the biometric information sharing program. The ARIES concept provides reporting and audit log details to assist with providing the facts surrounding the execution of the transmission that may or may not have disclosed the PII or the unauthorized access. Safeguards to assist in the monitoring and reporting of privacy incidents to DHS must be included in the policy or privacy documentation. In addition, foreign partners may have reporting obligations under their own laws.

The United States and the foreign partner require the representative parties to maintain a log of the transmission and receipt of data communicated to the other country. This log serves to:

[63] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS INSTRUCTION 047-01-001, PRIVACY POLICY AND COMPLIANCE (2011), *available at* https://www.dhs.gov/privacy-policy-guidance.

a) ensure effective monitoring of data protection in accordance with the national law of the respective country; b) enable the countries to effectively make corrections and block or delete certain data; c) inform the querying country of the result obtained from the supplied data; and d) ensure data security.

The log must include a) information on the data supplied; b) the date on which the data was supplied; and c) the recipient of the data in case the data is supplied to other entities.

The countries must protect the log with suitable measures against all forms of inappropriate use. Each country has stated their intent to carry out periodic quality assurance activities, including a review of applicable privacy safeguards, using a mutually decided methodology to ensure that the activities carried out under the international data sharing initiative are consistent with its terms. These activities may include determining whether information:

- Has been retained when it should have been destroyed;
- That was exchanged under the biometric information sharing program has been marked as having been received from the partner;
- Has been disclosed in a manner inconsistent with the biometric information sharing program; and
- Has been corrected in a manner consistent with the biometric information sharing program.

Information such as the number of transactions, biometric match statistics, and transactional metadata are accumulated in the audit log to ensure that informational statistics are always available to inform compliance requirements.

ISAAs listed in the Appendix, except for BITMAP, contain language that the participating countries agree to notify the other promptly, but no later than 48 hours after becoming aware of any unauthorized access, use, disclosure, modification, or disposal of information received under the governing cooperative statement. Each participating country is obligated under the terms of the ISAA to furnish all necessary details of the unauthorized access, use, disclosure, modification, or disposal of that information as appropriate.

Consultations on any privacy incidents involving PII, including unauthorized access or disclosure, as well as remedial actions taken in response to any such incidents, may be outlined in the cooperative statements between the U.S. Government agency and the foreign partner agency. ARIES will provide any data analysis, audit log information, or transactional data that is relevant to support the analysis of any privacy incident identified by either party.

Responsible Official

Craig Kelly
Privacy Officer
Office of Biometric Identity Management
Management Directorate
U.S. Department of Homeland Security

Kenneth Gantt
Deputy Director
Office of Biometric Identity Management
Management Directorate
U.S. Department of Homeland Security
(202) 298-5200

Approval Signature

Original, signed copy on file at DHS Privacy.

_____

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

Appendix A: Source Privacy Compliance Documentation

U.S. Customs and Border Protection (CBP)

CBP PIAs: https://www.dhs.gov/privacy-impact-assessments.

- DHS/CBP/PIA-002 Global Enrollment System (GES) and *subsequent updates*;
- DHS/CBP/PIA-006 Automated Targeting System (ATS) and *subsequent updates*;
- DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative and *subsequent updates*;
- DHS/CBP/PIA-012 CBP Portal (e3) to EID/IDENT and *subsequent updates*;
- DHS/CBP/PIA-021 TECS System: Platform;
- DHS/CBP/PIA–024 Arrival and Departure Information System and *subsequent updates*;
- DHS/CBP/PIA-026 Biometric Exit Mobile Program and *subsequent updates*;
- DHS/CBP/PIA-051 Automated Passport Control (APC) and Mobile Passport Control (MPC); and
- DHS/CBP/PIA-056 Traveler Verification Service.

CBP SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/CBP-002 Global Enrollment System, 78 FR 3441 (Jan. 16, 2013);
- DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012);
- DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (Dec. 13, 2016);
- DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 FR 77753 (Dec. 19, 2008);
- DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);
- DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (Nov. 18, 2015); and
- DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (Oct. 20, 2016).

Immigration and Customs Enforcement (ICE)

ICE PIAs: https://www.dhs.gov/privacy-documents-ice.

- DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) and *subsequent updates*;
- DHS/ICE/PIA-003 electronic Travel Document System;
- DHS/ICE/PIA-009 Fugitive Case Management System (FCMS);
- DHS/ICE/PIA-011 Visa Security Program Tracking System and *subsequent updates*;
- DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and *subsequent updates*;
- DHS/USCIS/PIA-020 Alien Criminal Response Information Management System (ACRIMe) and *subsequent updates*;
- DHS/ICE/PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management Systems; and
- Forthcoming Biometric Identification Transnational Migration Alert Program (BITMAP) PIA.

ICE SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/ICE 001 Student and Exchange Visitor Information System, 75 FR 412 (Jan. 5, 2010);
- DHS/ICE-006 Intelligence Records System (IIRS), 75 FR 9233 (Mar. 1, 2010);
- DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 FR 20844 (May 8, 2018);
- DHS/ICE-009 External Investigations, 85 FR 74362 (Nov. 20, 2020);
- DHS/ICE-010 Confidential and Other Sources of Information, 78 FR 7798 (Feb. 4, 2013);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016); and
- DHS/ICE-014 Homeland Security Investigations Forensic Laboratory, 81 FR 45523 (July 14, 2016).

U.S. Citizenship and Immigration Services (USCIS)

USCIS PIAs**:** https://www.dhs.gov/uscis-pias-and-sorns.

- DHS/USCIS/PIA-007 Domestically Filed Intercountry Adoptions Applications and Petitions and *subsequent updates*;

- DHS/USCIS/PIA-008 Enterprise Service Bus 2 (ESB 2) and *subsequent updates*;
- DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems and *subsequent updates*;
- DHS/ALL/PIA-027 USCIS Asylum Division and *subsequent updates*;
- DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals (DACA) and *subsequent updates*;
- DHS/USCIS/PIA-048 USCIS International Biometric Processing Services and *subsequent updates*;
- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS) and *subsequent updates*;
- DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS) and *subsequent updates*; and
- DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting.

USCIS SORNs: https://www.dhs.gov/system-records-notices-sorns.

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
- DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016);
- DHS/USCIS-007 Benefits Information System, 84 FR 54622 (Oct. 10, 2019);
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015);
- DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016); and
- DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018).

Department of State (DOS)

- STATE-26 Passport Records, 80 FR 15653 (March 24, 2015);
- STATE-36, Security Records, 83 FR 28058 (Jun. 15, 2018); and
- STATE-39 Visa Records, 83 FR 28062 (Jun 15, 2018).

Department of Defense (DoD)

- A0025-2 SAIS DoD Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009); and

- A0025-2 PMG (DFBA) DoD Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015).

Intelligence Community

- JUSTICE/FBI-019 Terrorist Screening Records System of Records, 76 FR 77847 (Dec. 14, 2011).

Department of Justice (DOJ) and state/local/tribal/territorial law enforcement, federal, state, local investigative agencies

- JUSTICE/INTERPOL-001 INTERPOL-United States National Central Bureau (USNCB) Records System, 75 FR 27821 (May 18, 2010) [Note: records shared with DHS include: law enforcement, intelligence, and national security records];
- JUSTICE/DOJ-005 Nationwide Joint Automated Booking System, 72 FR 3410 (Jan. 25, 2007), 71 FR 52821 (Sept. 7, 2006); and
- JUSTICE/FBI-009 Next Generation Identification (NGI) System of Records, 81 FR 27284 (May 5, 2016).

The DHS Office of Strategy, Policy, and Plans is the Program Manager for information sharing with international partners, including Migration 5 partners Canada, New Zealand, Australia, and the United Kingdom. DHS also shares information with Greece and Mexico.

PIAs: https://www.dhs.gov/privacy-documents-department-wide-programs.

- Canada – IDENT Appendices https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system;
- New Zealand - IDENT Appendices https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system;
- Australia - IDENT Appendices https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system;
- United Kingdom - IDENT Appendices https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system;
- Mexico - IDENT Appendices https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system; and
- DHS/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy https://www.dhs.gov/publication/dhsallpia-064-preventing-and-combating-serious-crime-pcsc-agreements-greece-and-italy.