Privacy Impact Assessment

for the

Biometric Identification Transnational Migration Alert Program (BITMAP)

DHS Reference No. DHS/ICE/PIA-065

March 17, 2025

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations (HSI) established the Biometric Identification Transnational Migration Alert Program (BITMAP) to promote and strengthen the international cooperation and coordination of law enforcement agencies' efforts to combat transnational criminal activity, identify threats of potential terrorism, and enforce customs laws. Through BITMAP, foreign law enforcement partners[1] share with the United States biometric and biographic information they collect within their borders on foreign nationals whom they reasonably suspect of being involved in terrorism-related activity or posing an immigration, criminal, or international security risk. In response to the information the United States receives from the foreign partner, the United States then may share, on a case-by-case basis, relevant derogatory information of investigative value about the subject individual with the foreign partner. This Privacy Impact Assessment (PIA) provides transparency into how BITMAP leverages biometric and biographic information as part of ICE's effort to detect and dismantle transnational criminal and terrorist networks that pose a risk to the United States. This Privacy Impact Assessment also describes how the exchange of information between ICE and its foreign law enforcement partners employs safeguards to protect privacy and civil liberties in accordance with law, regulation, and policy.

Introduction

BITMAP is a host-country-led initiative in which HSI trains and equips foreign law enforcement partners to collect biometric and biographic data on individuals suspected of transnational criminal or terrorism ties. Biometric data is measurable biological (anatomical or physiological, such as fingerprints) or behavioral characteristics used for identification of an individual. Once a biometric or biographic match is established, any subsequent sharing of information provides useful investigative leads and supports future identity verification for both the United States and the foreign partner.

Foreign partners share with HSI their collected data, which HSI screens and enters into a U.S. Government database. This biometric and biographic data exchange with foreign partners contributes to United States security by reducing the likelihood of onward travel to the United States of actors, criminals, and undocumented individuals who threaten national security, and promotes the integrity of legitimate global travel and migration. HSI special agents assigned to

[1] For purposes of this Privacy Impact Assessment, the term "foreign law enforcement partner" or "foreign partner" refers to the foreign country's law enforcement agency or entity participating in the program, not a specific individual or device.

foreign posts – called Attachés -- collaborate with host nation law enforcement partners on mutual investigative targets, including conducting joint counterterrorism, enforcement, and training operations.

BITMAP operates under 19 U.S.C. § 1628 and in support of Executive Orders[2] and Presidential Directives[3] written to strengthen cooperation and facilitate the exchange of information between foreign and domestic law enforcement agencies with authorized access to information maintained in DHS systems.[4] BITMAP observes all U.S. obligations under applicable bilateral and multilateral treaties and agreements, including the protection of personal information. BITMAP collections are used in activities that align with HSI's legal authorities and mission to protect U.S. borders, national security, and public safety by investigating, disrupting, and dismantling transnational criminal organizations that engage in all types of smuggling and trafficking, including human, narcotics, money, weapons, and sensitive technologies.

---

[2] *See* Executive Order 14165, *Securing our Borders* (90 Fed. Reg. 8467, January 20, 2025), *available at* https://www.federalregister.gov/documents/2025/01/30/2025-02015/securing-our-borders; Executive Order 13773, *Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking* (82 Fed. Reg. 10691, February 9, 2017), *available at* https://www.federalregister.gov/documents/2017/02/14/2017-03113/enforcing-federal-law-with-respect-to-transnational-criminal-organizations-and-preventing; and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (70 Fed. Reg. 62023, October 25, 2005), *available at* https://www.federalregister.gov/documents/2005/10/27/05-21571/further-strengthening-the-sharing-of-terrorism-information-to-protect-americans.

[3] *See* HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-6, *Integration and Use of Screening Information to Protect Against Terrorism* (September 16, 2003), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf; HSPD 11, *Comprehensive Terrorist Related Screening Procedures* (August 27, 2004), *available at* https://www.hsdl.org/?abstract&did=449327; and HSPD 24/NATIONAL SECURITY PRESIDENTIAL DIRECTIVE (NSPD) 59, *Biometrics for Identification of Screening to Enhance National Security* (June 5, 2008), *available at* https://www.hsdl.org/?abstract&did=486560.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM), PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim. IDENT is soon to be replaced with the Homeland Advanced Recognition Technology system (HART) as the DHS-wide biometric database that stores and processes biometric data and links biometrics with biographic information to establish and verify identities. For purposes of this Privacy Impact Assessment, this system will be referred to as "IDENT" for simplicity. Also, *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, and *see* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM), PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART), DHS/OBIM/PIA-004 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

BITMAP's Arrangements with Foreign Partners

HSI establishes BITMAP operations in a foreign country in coordination with and with concurrence from the U.S. Department of State (DOS). A foreign government, another DHS entity, or a domestic law enforcement partner (e.g., Federal Bureau of Investigation (FBI)) may affirmatively request foreign partner participation in BITMAP. In coordination with HSI managers, the BITMAP project managers employ a site selection methodology to identify foreign law enforcement partner agencies suitable for BITMAP. BITMAP's site selection process may be modified to support the program's operational needs and ensure adherence to law, regulation, or policy including:

- *Risk-based Country Evaluation*. Assessment of several crime-related risk factors (e.g., the number of transnational criminal organizations and gangs operating within a country) to identify countries that pose the highest risk to public safety and security.
- *Threat and Criminal Investigations Intelligence Assessment*. Intelligence analysis of current U.S. Government reporting, intelligence, and investigations to ensure the operational value and feasibility of establishing BITMAP operations to effectively address emerging threats in the region.
- *Capabilities and Partner Nation Assessments*. The responsible Attaché must have adequate ICE personnel, known as "BITMAP Advisors," to support and coordinate training and oversight. Further, the BITMAP foreign partner must dedicate sufficient resources for BITMAP operations upon implementation.
- *Biometric Proposal*. In accordance with DHS Homeland Security Presidential Directive 24 (HSPD-24),[5] federal agencies are required to complete a proposal to coordinate biometric sharing programs and obtain concurrence from the U.S. Embassy in the host country. This requirement ensures U.S. federal agencies are not duplicating efforts and deconflicts international engagements.
- *Human Rights Vetting*. The Department of State is responsible for independently vetting the foreign law enforcement partner (i.e., the security force unit) and each unit's law enforcement official to determine whether there is a pattern of human rights violations. Vetting begins in the unit's home country, where the U.S. Embassy conducts consular, political, and other security and human rights checks. The Department of State Bureau of Democracy, Human Rights, and Labor (DRL) evaluates all available information about the

[5] *See* Homeland Security Presidential Directive 24: Biometrics for Identification of Screening to Enhance National Security (June 5, 2008), *available at* https://www.hsdl.org/?abstract&did=486560.

human rights records of the unit and each unit's law enforcement official.[6] The Department of State will not concur with the BITMAP participation of a foreign partner if there is credible information implicating the foreign partner or its official in the commission of gross violations of human rights, and HSI will not deploy BITMAP to that foreign partner.

Attaché Roles and Responsibilities.

Attachés maintain ICE international offices and report to ICE and directly to the Ambassador in their host country. Their primary duties include relationship building, operational and investigative activity, repatriation efforts, training, and outreach on ICE international priorities. The Attaché offices also coordinate international investigations; acquire and develop cross-border criminal activities intelligence involving people, goods, and technologies, and provide investigative support to ICE domestic offices in combating transnational crime. HSI Attachés are responsible for the ICE relationship with the law enforcement partners in the country and continually assess the relationship, support, and engagement of the country. The Attaché mentors the foreign partner through the entire deployment process of BITMAP. The Attaché also evaluates, in an ongoing process, the compliance and coordination with the foreign partner. This overarching analysis of the relationship is ongoing, and any misuse would lead to termination of the program. If there is a need, certain functionalities of the program can shut down. For example, the BITMAP devices (explained later) can be deactivated remotely, terminating access.

The Attachés and BITMAP Advisors receive the following BITMAP training:

- Overview of the BITMAP analytical process;
- The BITMAP enrollment process;
- Biometric collection device use and troubleshooting procedures;
- Legal and policy interpretation applicable to the program;
- Program law enforcement objectives compatible with the purposes for collection;
- Investigative action and accountability;
- Match notification procedures; and

[6] 22 U.S.C. § 2378d. Commonly called "The Leahy law," this statute prohibits the U.S. Government from using funds for assistance to units of foreign security forces where there is credible information implicating that unit or official in the commission of gross violations of human rights. Under the Foreign Assistance Act of 1961, the Department of State is responsible for conducting consular, political, and other security and human rights checks of foreign partners that are designated to receive assistance (e.g., resources, funds) from a U.S. federal agency.

- Annual DHS Privacy and Security Training.[7]

The responsible Attaché and BITMAP advisors overseeing each BITMAP deployment provide training to the foreign partners as follows:

- Device maintenance and use (e.g., software upgrades);
- Identification of transnational criminal and terrorism related activities;
- Basic interview and investigative techniques;
- Human rights principles and norms aligned with the seven major international human rights treaties;[8]
- and law enforcement standards and principles aligned with the United Nations Code of Conduct for Law Enforcement Officials.[9]

In addition to the Attachés' and BITMAP Advisors' oversight of the foreign partners, as discussed above, the foreign partners are taught how to use the nation-specific Targeting Selection Criteria by tagging the data with foreign partner identifier and one of the following four codes, which were derived to cover the range of persons captured within BITMAP and record the reason for enrollment:

- International and National Security: This code applies to non-U.S. persons[10] who may pose an international or national security risk to the United States, or its foreign partners based on the foreign partners' intelligence of the individual's terrorism-related activity, or information obtained during regular or irregular migration activity.
- Gang Members: This code applies to non-U.S. persons associated with a gang or gang member known for criminal activity (e.g., MS-13). Foreign law enforcement partners apply their regional knowledge to identify gang members.

[7] The ICE Office of Information Governance & Privacy will review modified course content or additional training materials developed by HSI or the BITMAP Project Management Team before changes are instituted.
[8] The seven major international human rights treaties are: (1) International Convention on the Elimination of All Forms of Racial Discrimination; (2) International Covenant on Civil and Political Rights; (3) International Covenant on Economic, Social and Cultural Rights; (4) Convention on the Elimination of All Forms of Discrimination against Women (CEDW); (5) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; (6) Convention on the Rights of the Child; and (7) Convention on the Rights of Persons with Disabilities. For more information, *see* www.treaties.un.org.
[9] *Available at* www.un.org/ruleoflaw/blog/document/code-of-conduct-for-law-enforcement-officials.
[10] A U.S. person is defined as a U.S. citizen or lawful permanent resident. 22 U.S.C. § 6010.

- Persons of Interest (POI): A Person of Interest code is selected for non-U.S. persons[11] suspected of criminal activity that would reasonably be considered felonious under U.S law, or who have been convicted of certain crimes (e.g., fraudulent documents, or money laundering).[12]
- Vetting: A vetting code is used for individuals known or suspected of being a U.S. person[13] or host nation national but whose information the BITMAP foreign partner does not want to have retained in U.S. Government biometric databases. These encounters are coded as search and non-retain, and the biometrics and biographical data are not retained.

The foreign partners must select the code that corresponds to one of the above four categories of individuals when submitting a BITMAP encounter, or their attempted submission is automatically rejected. This selection requirement ensures BITMAP encounters are properly linked and traceable to the foreign partner for audit purposes and aligned with BITMAP's law enforcement objectives.

The systems that enroll BITMAP encounters inform users that no adverse action should be taken based solely on the existence of a BITMAP encounter, which itself does not constitute derogatory information; and that it may not be used to deny a benefit or justification for taking adverse action on a benefit.[14]

Overview of the BITMAP Process and Data Lifecycle

The following steps outline the end-to-end process of BITMAP foreign partner selection and information exchange.

[11] *Available at* www.un.org/ruleoflaw/blog/document/code-of-conduct-for-law-enforcement-officials.
[12] Persons of Interests may include individuals who are reasonably suspected of a crime, are the subject of investigative interest based on the individuals' association with illegal cross-border activity or another criminal network, such as terrorist groups wanted in connection with a crime (e.g., arrest warrant), or there is investigative evidence linking the individual to criminal acts (e.g., bombing). This does not mean that all Persons of Interests are "terrorists," but rather that the travel and behavior of such individuals indicates a possible nexus to nefarious activity (including terrorism) and, at a minimum, provides indicators that necessitate heightened screening and further investigation.
[13] BITMAP foreign partners are prohibited from enrolling U.S. persons presenting valid U.S. travel documents, unless: (1) there are reasonable grounds for the foreign partner to suspect the identity documents may be fraudulent, such as at a foreign port of entry; (2) exigent circumstances (e.g., officer safety, natural disaster, the identification of human remains); or (3) immediate identification is needed for purposes of a criminal investigation of an offense for which such person is reasonably suspected in the host country, or involvement in criminal activity that is compatible with the program system collection.
[14] A BITMAP encounter, in and of itself, does not indicate the existence of derogatory information, similar to U.S. Customs and Border Protection (CBP) border crossing data. Were there to be derogatory information identified through the subsequent investigative and intelligence efforts by the United States or the foreign partner, then that information would be documented within the appropriate databases.

- **Step 1**: Currently, the foreign law enforcement partner expresses intent either verbally or via a non-binding written request to participate as a BITMAP foreign partner. The Department of State Chief of Mission assigned to the region provides concurrence of BITMAP's intent to deploy with the foreign law enforcement partner. The current countries that are active on BITMAP are doing so under Title 19 Section 1628 Law Enforcement Sharing authorities which are documented in Customs Mutual Assistance Agreements or previously established Information Sharing Agreements that are not specifically tailored to BITMAP requirements. It has been identified that various information sharing regimes, such as General Data Protection Regulation (GDPR), require a more formal agreement. In these cases, the foreign partner will have a formal written Information Sharing Agreement in place before sharing any information. Where relevant, the Preventing and Combatting Serious Crime (PCSC) agreement format, which was used to draft the Internal Security Agency agreement between ICE and Poland, for example, will be used.
- **Step 2**: BITMAP provides the foreign law enforcement partners with training and biometric devices used to collect and submit BITMAP encounters. The biometric devices allow the BITMAP foreign partner to collect the necessary biometrics (e.g., fingerprints) and biographic information (e.g., name, place of birth, sex) pertaining to individuals who fall within the BITMAP Targeting Selection Criteria. The BITMAP foreign partner may also enter encounter information, which is relevant data obtained during their investigation. The foreign partner is required to select from the Targeting Selection Criteria dropdown menu the category of individual they encountered in accordance with the Targeting Selection Criteria.
- **Step 3**: The BITMAP foreign partner submits the BITMAP encounter to DHS via a secure (and encrypted) one-way portal, the CBP Unified Passenger (UPAX) system.[15] The CBP Unified Passenger system receives the information, converts it into the appropriate format, and automatically sends the data to the following three U.S. Government databases to determine if there is a match:
    - The DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT);[16]

[15] The CBP Unified Passenger system is a function within CBP's Automated Targeting System.
[16] BITMAP encounter information first gets transmitted to IDENT, which in turn provides the information to FBI Next Generation Identification (NGI), which then transmits the applicable information to the Department of Defense (DoD) Automated Biometric Information System (ABIS). *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM), PRIVACY IMPACT ASSESSMENT FOR THE

        - At this point, IDENT automatically checks each encounter against the U.S. Citizenship and Immigration Services (USCIS) Central Index System[17] to remove any records pertaining to a member of a Special Protected Class.[18]
    - The Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) system;[19] and
    - The Department of Defense (DoD) Automated Biometric Identification System (ABIS).[20]

- **Step 4:** Once the three U.S. Government databases receive this information, the BITMAP encounter is considered "enrolled" and the information will be retained in accordance with each agency's records retention schedule (except for encounters under the vetting code whose biographic and biometric data are not retained or in instances where retention is

AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim. DHS is in the process of replacing IDENT with the Homeland Advanced Recognition Technology System as the primary DHS system for storage and processing of biometric and associated biographic information. See U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), available at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (CIS), DHS/USCIS/PIA-009 Central Index System, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[18] Special Protected Class is defined as persons for which there are additional statutory, regulatory, or policy confidentiality protections. Information pertaining to these persons may require special handling and safeguarding. The persons covered under this definition include, but are not limited to, Asylum-Seekers, Asylees, and Refugees; petitioners for victim-based relief or benefits (VAWA, T Visa, and U Visa); individuals with Temporary Protected Status; S Visa holders; Legalization and Legal Immigration Family Equity (LIFE) Act applicants; and Special Agricultural Worker program applicants. All BITMAP encounters are automatically screened against DHS databases to check for Special Protected Class protections before enrollment into external U.S. Government biometric databases (e.g., DoD Automated Biometric Information System) to prevent the inadvertent disclosure of sensitive information. Special Protected Classes are removed from onward sharing at first enrollment within IDENT. Foreign partner encounters associated with a member of a Special Protected Class are not transmitted to other biometric databases and a foreign partner will not have any acknowledgement of the results. Any information linking a member of a Special Protected Class to criminal activity will be addressed manually and not in an automated fashion.

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

[20] For more information about DoD's Automated Biometric Identification System, *see* https://asc.army.mil/web/portfolio-item/biometric-enabling-capability-bec/.

further restricted, such as by a treaty).[21] BITMAP foreign partners do not have direct access to any U.S. Government database, nor to any of the information contained within such databases. All encounters enrolled in these databases are identified as "BITMAP" through the Targeting Selection Criteria dropdown codes for auditing and reporting purposes. More information on the BITMAP auditing process can be found in the "Auditing and Accountability" section below.

- **Step 5**: The U.S. Government databases identified above search their records and send an automated message back to the CBP Unified Passenger system as to the existence of a "match" or "hit." For example, if the DHS IDENT system identifies a match, the message might say, *this information matches an individual with IDENT number 1234567*.
- **Step 6**: All information sent back to the CBP Unified Passenger system from the three databases referenced above gets compiled into a "hot list," which is manually reviewed by a BITMAP analyst. Access to the hot list is granted on a "need to know" basis. The BITMAP analyst also manually reviews each BITMAP encounter to remove any records that should not be retained in certain U.S. Government databases and to conduct analysis in the appropriately secure environment.
- **Step 7**: ICE responds to the BITMAP foreign partner: a) This submission is complete; b) Please contact your assigned BITMAP Advisor; or c) This submission is still in processing. A response will be sent once the submission is complete.
- **Step 8**: In the event of a match, DHS reviews U.S. Government holdings for information that is of investigative value and permissible to share with the foreign law enforcement partner. If relevant information is controlled by another U.S. agency, HSI will contact the agency to authorize sharing with the foreign law enforcement partner, according to any information sharing agreements or policies. DHS will then determine the most appropriate method to assist the foreign law enforcement partner. If the foreign law enforcement partner requires additional or formal documentation, they may submit a written request to the Attaché. The Attaché will determine what additional information is permissible for DHS to consider sharing information with the foreign partner, including the review and identification of derogatory information maintained in U.S. holdings to assess the potential investigative value of sharing. Information is shared with foreign partners in accordance

[21] BITMAP encounters using the "VET" category only include the date of encounter, time of encounter, and the name of any federal agency who conducted a query for that individual. This information is only maintained for auditing purposes.

with all applicable laws and regulations and complies with approved policies and guidelines at the Attaché post.

Onward Sharing by the Foreign Partner

Onward Sharing by the Foreign Partner under Title 19 Section 1628 and any needed agreements will be put in place to establish boundaries that are evaluated based on the ongoing relationship with the foreign country. The limitations generally establish the purpose of sharing as law enforcement and prohibit sharing to third parties.

Data Retention and Special Protected Classes

The U.S. Government databases will retain this data in accordance with their approved records retention schedules. Specific information pertaining to each agency's retention schedule (including a citation to the corresponding schedules) is detailed below in the "Data Minimization" section of this Privacy Impact Assessment.

BITMAP encounters are retained to support future queries against the information maintained in U.S. Government databases. Although this information is "enrolled" and retained by the three U.S. Government databases, each encounter contains a disclaimer specifying how this information should be treated. For example, a BITMAP encounter could indicate a foreign partner encounter as a Person of Interest. If so, the encounter would contain corresponding language, such as: *Foreign Partner encounter as a Person of Interest. This does not constitute derogatory information. Do not take action based on this record*. The disclaimer helps ensure that no adverse action is taken based on this information alone.

If information provided by the BITMAP foreign partner (using the *Vetting* code) pertains to a U.S. citizen, lawful permanent resident, or citizen of the host country, automatically the biographic and biometric data is not retained. Rather, these encounters are compared against the three U.S. Government databases via a search-only transaction. This prevents automatic enrollment and retention of these individuals' information in U.S. Government databases.

There may be circumstances in which a foreign partner submits an encounter involving a U.S. person mistakenly, using ana alternate code rather than the *Vetting* code (such as due to human error or because the U.S. person provided false identification). Under these circumstances, information maintained in U.S. Government databases may contain U.S. person identifiers that alert the BITMAP analyst or Attaché to a potential mis-identified foreign partner BITMAP enrollment. Unless there is a law enforcement purpose to retain the U.S. person encounter, ICE will manually remove any BITMAP encounter from all government biometric databases, and the foreign partner must re-submit the encounter using the *Vetting* code. Individuals have the

opportunity to provide accurate information about themselves to foreign law enforcement partners at the time of collection. If U.S. persons believe that the information maintained about them is inaccurate or improper, they can submit a request for review and correction following the redress instructions outlined further below.

Finally, ICE has established strict security and privacy access controls for BITMAP to safeguard against unauthorized access or the inappropriate disclosure of sensitive information. There are legal prohibitions that prevent ICE from providing certain information to domestic and foreign law enforcement partners. For example, there are strict non-disclosure requirements for an individual that belongs to a Special Protected Class, such as individuals seeking or granted relief under the Violence Against Women Act (VAWA) of 1994,[22] T-nonimmigrant status (victims of human trafficking), and U-nonimmigrant status (victims of qualifying crimes);[23] or individuals seeking or granted certain immigration benefits (e.g., asylum, refugee status). By law, these individuals are afforded additional confidentiality protections. ICE requires that the relevant ICE systems and programs, including BITMAP, establish a mechanism for identifying individuals to whom these confidentiality laws apply. When information is received by the CBP Unified Passenger system via the secure DHS one-way portal, the CBP Unified Passenger system searches its DHS systems to determine if any BITMAP encounters pertain to a member of a Special Protected Class. If so, the CBP Unified Passenger system does not send that information onward, and this information is not enrolled as a BITMAP encounter. This process helps ensure that BITMAP disclosures comply with all applicable laws, regulations, and departmental policies.[24] Information regarding the confidentiality of Special Protected Class records is discussed further in the "Principle of Security" section below.

Data Sharing with U.S. Government Agencies

Sharing with U.S. Department of Defense (DoD)

In 2011, DHS entered into a Memorandum of Agreement (MOA) with DoD for the exchange of biometric, biographic, contextual, and other identity management data related to screening people and identity verification. For purposes of BITMAP, ICE shares information with DoD in accordance with the 2011 Memorandum of Agreement which enhances the ability of both DoD and DHS (and its Components) to verify the identity of persons of interest and national

[22] 42 U.S.C. §§ 13701-14040.
[23] 8 U.S.C. § 1367 (Section 1367).
[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY DIRECTIVE 002-02, REV. 00.1, IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS (Apr. 29, 2019); U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY INSTRUCTION 002-02-001, IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS (Nov. 7, 2013), on file at the DHS Privacy Office.

security threats. Finally, ICE transmits BITMAP data to the DoD Automated Biometric Information System in a manner consistent with any overarching arrangements or agreements with the BITMAP foreign partner.[25]

Sharing with U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI)

In 2008, DHS entered into a Memorandum of Understanding (MOU) with both the FBI and Department of State for the exchange of biometric and biographic information retained by the parties via an automated interoperability process. This Memorandum of Understanding contemplates the exchange of data between DHS and FBI so that each party can inform the other regarding a match resulting from a query. The Memorandum of Understanding is on file with each agency. The shared BITMAP data serves the law enforcement mission needs of both agencies. ICE transmits BITMAP data to FBI's Next Generation Identification system in support of the parties' respective criminal law enforcement missions. HSI also shares BITMAP biometric data with the Department of State via IDENT, for which the Department of State has access.

BITMAP Use Case Examples

U.S. and foreign law enforcement partners use BITMAP as an investigative tool or mechanism to provide lead information for investigative inquiries; to assist in criminal investigations; to disrupt terrorist, terrorism-related, and transnational criminal activity; and to provide new opportunities to identify individuals who fit one of the targeting categories described above (e.g., Person of Interest). Below are several examples of how DHS Components, including ICE, and domestic and foreign law enforcement use the information the BITMAP foreign partners provide to assist in each entity's respective law enforcement investigations:

- Supporting U.S. efforts in visa vetting and the admission decision-making process.
- Disrupting and dismantling Transnational Criminal Organizations and criminal networks, such as drug cartels that create and maintain illicit pathways across borders to smuggle illegal goods that are used by secondary criminal networks. For example, HSI and CBP use BITMAP information and coordinate with foreign and domestic law enforcement partners to target transnational criminal infrastructure and associates.
- Documenting the movement of suspect individuals to facilitate and enhance the quality and timeliness of immigration and admissibility decisions by U.S. law enforcement and other government officials.

[25] If the BITMAP foreign partner is a member of the European Union, for example, information sharing would be consistent with the requirements of the Data Protection and Privacy Agreement (DPPA) between the United States and European Union (EU).

- Associating derogatory information with known or suspected criminals during law enforcement investigations. A U.S. law enforcement agent may use BITMAP information to discover connections among law enforcement and government investigations. For example, a U.S. government agency collects a latent fingerprint from bomb-making material and enters it into a U.S. government biometric database to find potential matches. That latent print would be identified as belonging to a Person of Interest and retained in U.S. Government biometric databases. Independently, the BITMAP foreign partner may encounter the individual during an investigation for an offense that occurred in the foreign partner's jurisdiction and provide the print to the United States for identification through the Targeting Selection Criteria. The United States now has more information on the individual who left the latent print on the bomb-making material and the information sharing furthers U.S. national security interest. Any sharing back of information to the foreign partner, if appropriate, would also further international security interests.
- BITMAP is used to make nominations to the Terrorist Screening Database (TSDB) to determine suitability.[26] Specially trained analysts assess whether BITMAP data should be used to nominate to the Terrorist Screening Database and make the appropriate information available to the Terrorist Identities Datamart Environment (TIDE).[27]
- The Attaché offices will use BITMAP information to provide investigative support as part of the primary duties of the in-country Attaché, such as acquiring and developing intelligence-related cross-border criminal activity and coordination of international investigations between all U.S. foreign partners.[28]

Examples of use cases documenting HSI's proactive oversight include:

- When a foreign law enforcement partner's BITMAP encounter results in a match to an individual with a U.S. warrant, the Attaché will notify the appropriate U.S. Government agency to confirm prosecutorial interest. Once confirmed, the Attaché will facilitate coordination between the relevant U.S. Government agency and the foreign law enforcement partner. If the warrant is notified through the International Criminal Police

[26] The Terrorist Screening Database is owned by the FBI's Threat Screening Center (TSC). For more information about the Terrorist Screening Database, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE WATCHLIST SERVICE, DHS/ALL/PIA-027 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[27] For more information about the Terrorist Identities Datamart Environment, *see* https://www.dni.gov/files/NCTC/documents/features_documents/TIDEfactsheet10FEB2017.pdf.
[28] Any sharing of CBP-owned information is done so in accordance with the memorandum of authorization between ICE and CBP. This memorandum also outlines how such disclosures are documented and how each biometric system will maintain a record of any disclosures of information.

Organization (INTERPOL), the Attaché will help facilitate the detention of the suspect individual and coordinate communication between the BITMAP foreign partner and INTERPOL will notify the country/agency originating the warrant.

- A known gang member may be of investigative interest to another BITMAP foreign partner or foreign country (not a BITMAP foreign partner) operating in transit destination points (i.e., illegal activity located between countries). In this case, an Attaché representative will conduct follow-up actions and communicate with foreign partners and other lawfully interested parties to facilitate the sharing of investigative information in accordance with applicable laws, regulations, policies, and treaty obligations.
- An individual presents a false identity document that the BITMAP enrollment discovers is a match to a known human smuggler. The Attaché would coordinate with the foreign law enforcement partner to share the associated investigative information related to the matched information as well as any related human smuggling network information. From there, all parties can work to further the potential investigative leads.
- Finally, ICE may also share BITMAP information with other U.S. federal agencies operating in the area that have an investigative interest and for deconfliction purposes, to avoid interfering in another agency's on-going law enforcement investigation(s) and/or operation(s).

Retroactive identification and removal of improper enrollments

If a subject is inadvertently enrolled (e.g., a U.S. person is enrolled with the wrong code), a duplicate enrollment, or there is a subsequent identification of an U.S. person (including lawfully permanent residents), the BITMAP analyst team submits a Delete Request to the DOD Automated Biometric Identification System, DOJ Next Generation Identification, DHS IDENT, and CBP Unified Passenger system to delete the file. All agencies respond when deletion is complete. The file will no longer exist in the U.S. Government databases.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[29] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(2) states that the Chief Privacy Officer shall assure

[29] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[30]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[31] The Fair Information Practice Principles account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208,[32] and the Homeland Security Act of 2002, Section 222.[33] Given that BITMAP is a program rather than a particular information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the privacy impact of BITMAP as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

ICE provides public transparency through the issuance of this Privacy Impact Assessment, which describes how BITMAP promotes and strengthens the international cooperation and coordination of law enforcement agencies' efforts to combat transnational criminal activity, identify threats of potential terrorism, and enforce customs laws. ICE is also informing the public about how BITMAP provides meaningful technical assistance to foreign law enforcement partners that lack resources to effectively share law enforcement and intelligence information with the United States. Through BITMAP, foreign law enforcement partners share with the United States biometric and biographic information they collect within their borders on foreign nationals whom they reasonably suspect of being involved in terrorism-related activity or posing an immigration, criminal, or international security risk. Such information provides valuable investigative leads that assist the efforts of DHS Components and domestic law enforcement partners to counter criminal

[30] 6 U.S.C. § 142(a)(2).
[31] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE U.S. DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[32] 44 U.S.C. § 3501 note.
[33] 6 U.S.C. § 142.

acts, such as terrorism.

DHS also provides transparency through the Privacy Impact Assessments for DHS/OBIM/PIA-001 Automated Biometric Identification System[34]/DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART),[35] to inform the public that DHS data eventually may be shared in response to a matching query from a foreign partner. In addition to the IDENT/HART systems, ICE may retain BITMAP records in its own systems based on the circumstances of the case. For example, if ICE undertakes a separate criminal investigation for an individual identified through BITMAP, that person's information would be maintained in the ICE Investigative Case Management System (ICM).[36] Any records that ICE uses for link analysis may also be retained in the Repository for Analytics in a Virtualized Environment (RAVEN).[37] Transparency is be provided by those systems' corresponding Privacy Impact Assessment documentation.

In addition, DHS provides transparency through the relevant System of Records Notice(s) (SORN) covering the IDENT/HART sources, as follows:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, which covers records documenting ICE's criminal arrests, and most of ICE's immigration enforcement actions;[38]
- DHS/CBP-006 Automated Targeting System, which supports CBP in identifying individuals and cargo that need additional review traveling to and from the United States;[39]

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

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

[36] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT (ICM) SYSTEM, DHS/ICE/PIA-045(a) (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[37] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN), DHS/ICE/PIA-055 (2020), *available at* https://www.dhs.gov/privacy-documents-ice.

[38] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 89 FR 55638 (July 5, 2024), *available at* https://www.dhs.gov/system-records-notices-sorns.

[39] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, which covers the collection, use, and storage of biometric and biographic data for background checks and its results; it also covers background checks and their results;[40]
- DHS/ALL-041 External Biometric Records, which covers the maintenance of biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities;[41] and
- DHS/ALL-043 External Biometric Administrative Records, which covers technical and administrative information necessary to carry out functions that are not explicitly outlined in component source-system System of Records Notices, such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.[42]

Privacy Risk: There is a risk that individuals may not receive adequate notification about the collection and uses of their information, or how information is maintained or disseminated when providing biometric or biographical data to a foreign law enforcement partner.

Mitigation: This risk is partially mitigated. ICE provides general notice of BITMAP through its public-facing website.[43] Further, both DHS and ICE provided information to the public regarding the purpose and operations of BITMAP.[44] ICE provides notice that DHS data eventually may be shared in response to a matching query from a foreign partner or retain BITMAP records in its own systems through publication of ICE and DHS Privacy Impact Assessment(s) and System

[40] *See* DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), 83 FR 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[41] *See* DHS/ALL-041 External Biometric Records (EBR), 83 FR 17829 (April 24, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[42] *See* DHS/ALL-043 External Biometric Administrative Records (EBAR), 85 FR 14955 (March 16, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[43] *See* https://www.ice.gov/about-ice/hsi/our-offices/hq/bitmap.
[44] *See* written testimony of ICE Homeland Security Investigations International Operations Assistant Director Raymond Villanueva for a House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence hearing title "Combating Transnational Gangs Through Information Sharing," *available at* https://www.dhs.gov/news/2018/01/18/written-testimony-ice-house-homeland-security-subcommittee-counterterrorism; *see also* U.S. Immigration and Customs Enforcement Statement of Derek Benner, Acting Deputy Director of ICE testified before the U.S. Senate Committee on Homeland Security and Governmental Affairs regarding BITMAP's role in the migration crisis, *available at* https://www.hsgac.senate.gov/imo/media/doc/Testimony-Benner-2019-11-13.pdf.

of Records Notice(s).[45]

This risk is also partially mitigated through the publication of this Privacy Impact Assessment, as well as the publication of Privacy Impact Assessment(s) and System of Records Notice(s) listed above, addressing the collection, notification, and sharing of biometric and biographic information.

However, this risk cannot be fully mitigated because the original data is collected by the foreign partners in their jurisdiction.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Due to the law enforcement purpose of BITMAP, a traditional approach to individual participation is not always practical or possible when sharing information with law enforcement agencies. It would be counterproductive to provide subjects with access to certain investigative information about themselves during a pending law enforcement or security investigation, as this would alert them to, or otherwise compromise, the investigation. Although individuals may not always participate in the collection of information about themselves shared pursuant to an investigation or other law enforcement action or access such records during a pending law enforcement investigation, individuals may contest or seek redress during any resulting prosecution or proceedings brought against them by the United States or through appropriate redress measures made available by a BITMAP foreign partner. In addition, U.S. citizens and Lawful Permanent Residents have the right to request amendment of records under the Privacy Act of 1974.[46] The Judicial Redress Act extends certain rights of judicial redress established under the Privacy Act to citizens of covered countries. The Judicial Redress Act enables covered persons to sue for civil damages for willful and intentional disclosures of covered records made in violation of the Privacy Act.[47] Some BITMAP foreign partner countries are covered countries for the

[45] For example, if ICE undertakes a separate criminal investigation for an individual identified through BITMAP, that person's information would be maintained in the Investigative Case Management System. Any records that ICE uses for link analysis may be retained in the Repository for Analytics in a Virtualized Environment (RAVEN). Privacy Impact Assessments (and associated System of Records Notice(s)) for these systems are *available at* https://www.dhs.gov/privacy-documents-ice.

[46] 5 U.S.C. §552a.

[47] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017,

purposes of the Judicial Redress Act.

The Privacy Unit in the ICE Office of Information Governance & Privacy accepts record amendment requests from individuals covered by the Privacy Act. Individuals seeking notification of and access to any of the records covered by this Privacy Impact Assessment may submit a request electronically based on guidance at https://www.ice.goc/foia or in writing to the ICE Freedom of Information Act Officer at the below address:

U.S. Immigration and Customs Enforcement
Office of Information Governance & Privacy
Attn: Freedom of Information Act Unit
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(866) 633-1182
http://www.ice.gov/foia/

Individuals seeking to correct records contained in the appropriate system of records, or seeking to contest its content, may submit a request in writing to the ICE Privacy Unit:

U.S. Immigration and Customs Enforcement
Office of Information Governance & Privacy
Attn: Privacy Division
500 12th Street SW, Stop 5004 Washington, D.C. 20536-5004
http://www.ice.gov/about-ice/management-administration/privacy

Some of the requested information may be exempt from access pursuant to the Privacy Act or Judicial Redress Act to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory violation investigation or reveal an investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

Finally, DHS Privacy Policy makes clear that there is an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain

include the European Union (EU) and most of its member states. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website, *available at* https://www.justice.gov/opcl/judicial-redress-act-2015.

accurate records serves to undermine efficient decision making by DHS personnel and can create the risk of errors made by DHS and its personnel.

To that end, individuals not covered by the Privacy Act, or the Judicial Redress Act, may individually request access to their records by filing a Freedom of Information Act (FOIA) request with the respective component or DHS Freedom of Information Act office. Additional information about the Freedom of Information Act is available at https://www.dhs.gov/foia.

Privacy Risk: There is a risk that foreign partners will collect biometric and biographic information and provide it to DHS without individuals' knowledge.

Mitigation: This risk is partially mitigated. Due to the law enforcement purpose of BITMAP, individuals do not have an opportunity to consent or opt out of the program's collection and use of their information. It would be incumbent upon the foreign partner to provide any direct notice to these individuals. This Privacy Impact Assessment provides some measure of notice that the data collected by foreign partners may be maintained in U.S. Government systems.

Privacy Risk: There is a risk that individuals from whom biometrics are collected will have limited opportunity to correct their data due to the law enforcement sensitivity of the program and ICE system(s) or may not be aware how to make such requests for access or correction.

Mitigation: This risk is partially mitigated. Individuals whose information was processed pursuant to a BITMAP information sharing agreement (informal or formal) or that believe that the biometric information maintained about them is inaccurate or is the result of an improper BITMAP collection, may seek to access, correct, amend, or expunge information maintained in DHS systems, or otherwise seek redress from those foreign partners for the processing of information abroad, through partner countries' applicable access and redress laws.

Otherwise, individuals may submit a redress or correction request directly to the OBIM Privacy Officer, who will work with ICE to properly respond. For records maintained in IDENT, U.S. citizens, Lawful Permanent Residents, and individuals with records covered by the Judicial Redress Act may direct all requests to contest or amend information to:

OBIM Privacy
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave, SE
Mail Stop: 0655
Washington, D.C. 20528-0655

Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment.

In addition, if an individual believes that the information maintained about them is inaccurate or is the result of an improper BITMAP collection, HSI has established correction protocols to remove a BITMAP encounter from U.S. Government database in which the BITMAP enrollment was shared. HSI personnel will remove the BITMAP encounter from DHS systems and contact the system owners of FBI's Next Generation Identification and DoD's Automated Biometric Identification System and have the improper BITMAP encounter removed from external U.S. Government databases.

If individuals are dissatisfied with the response to their redress inquiries, they 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 the following address:

Chief Privacy Officer/Chief Freedom of Information Act Officer
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528
Phone: 202-343-1743 or 866-431-0486
Fax: 202-343-4011
E-mail: foia@hq.dhs.gov

As with access, amendments may be limited pursuant to applicable Privacy Act exemptions asserted by DHS for its systems of records.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Legal Authorities

BITMAP is authorized under 19 U.S.C. § 1628 through the Secretary's delegation to the Director of ICE to share and exchange information with foreign law enforcement agencies in furtherance of compliance and assistance with U.S. and the foreign partner's laws and regulations; bilateral or multilateral agreements; investigations; and, in any judicial or quasi-judicial proceedings. Pursuant to the Homeland Security Act of 2002 (Pub. L. No. 107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The DHS Secretary delegated this authority to ICE in DHS Delegation Number 7030.2, *Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the U.S. Department of*

Homeland Security (January 30, 2003). Separate authorities govern information sharing with European Union member states and the DoD.[48]

Purposes of the BITMAP Program

HSI established BITMAP for the purpose of creating an information-sharing program, designed to facilitate cooperation with foreign partners and strengthen the effectiveness of U.S. domestic and foreign law enforcement action. BITMAP collections are used for activities related to immigration decision-making, law enforcement activities with a nexus to the U.S. border, deterring transnational crimes and organizations, countering terrorism, and preventing and detecting crimes considered felonies under U.S. law or which render an individual inadmissible under the Immigration Nationality Act (INA), by comparing biometric and biographic information encountered by law enforcement during border inspections or in the course of criminal investigations, against relevant identity records in addition to criminal and terrorist records. Information gleaned from this sharing is used to prevent, detect, and investigate crime, including assessing whether an individual is involved in transnational crime, presents a criminal or terrorism risk, and aids border and immigration-related decisions. These authorized law enforcement purposes are discussed throughout this Privacy Impact Assessment and in relevant information sharing agreements or arrangements negotiated with foreign partner governments. BITMAP foreign partners collect information based on the program's purposes for collection, which align with HSI's legal authorities identified above. BITMAP collects biometric and associated biographic information as authorized by Homeland Security Presidential Directive (HSPD) 24/National Security Presidential Directives (NSPD) 59, *Biometrics for Identification and Screening to Enhance National Security*; Homeland Security Presidential Directive 6, *Integration and Use of Screening Information to Protect Against Terrorism*; Homeland Security Presidential Directive 11, *Comprehensive Terrorist Related Screening Procedures*; Executive Orders in federal law enforcement investigations and mission operations, immigration and border management, and for intelligence and national security purposes.

Privacy Risk: There is a risk that BITMAP foreign partners will use the biometric collection devices for reasons incompatible with BITMAP's function and intent.

[48] If ICE enters into any arrangements with European Union member states, this information sharing relationship is also covered under the Data Protection and Privacy Agreement between the European Union and the United States. DHS is specifically authorized to share BITMAP information with DoD under the aforementioned Memorandum of Agreement between the Departments. DoD's use of BITMAP information is also compatible with Article 3(1) of the Data Protection and Privacy Agreement in fulfilling DoD's mission in the "detection and prevention of terrorism." Additionally, under Title 10 of the U.S. Code Chapter 15, DoD is required to provide "intelligence information relevant to drug interdiction or other civilian law enforcement matters" and is authorized to support U.S. federal law enforcement agencies in combating transnational organized crime. *See* 10 U.S.C. § 271(c); 10 U.S.C. § 284 (b)(8).

Mitigation: This risk is partially mitigated. BITMAP program implementation requirements, including training, promoting the proper use of equipment, as well as technical and privacy oversight mechanisms, ensure that foreign partners submit BITMAP encounters for purposes compatible with the program's law enforcement objectives.

BITMAP foreign partners are required to attend a training program established by HSI. While each foreign partner operates and collects information in accordance with the foreign partner's laws, regulations, and policies of their respective jurisdiction, HSI takes steps to promote best practices and deter violations through principle-based training and guidance. The training identifies the program's law enforcement objectives to ensure that the foreign partner's participation aligns with those objectives. For example, training provided to the foreign partners includes extensive examples of appropriate targeting and investigative criteria for BITMAP encounters, this includes transnational criminal activity or other terrorism-related activity.

In addition, the training includes how to use the biometric collection devices, and the Targeting Selection Criteria a foreign law enforcement partner must use to identify suspect individuals. The Targeting Selection Criteria identifies four categories of individuals targeted in furtherance of the program's law enforcement objectives. The BITMAP foreign partner is required to use the biometric collection devices to select one of the four codes (i.e., International and National Security, Person of Interest, Gang Members, Vetting), which is associated with one of the four categories of individuals and purpose for collection. A BITMAP foreign partner enrollment that fails to have a corresponding Targeting Selection Criteria category is automatically rejected during the submission process and not retained in U.S. Government systems.

Finally, the Targeting Selection Criteria codes also identify the BITMAP foreign partner that submitted the enrollment. This allows the responsible Attaché to maintain oversight into the foreign partner's use of the biometric collection devices and review all BITMAP foreign partner enrollments and the corresponding codes. Any intentional deviation that is confirmed by BITMAP Advisors will result in corrective measures up to or including the exclusion of the foreign partner from the program and termination of the entire BITMAP initiative within the host country. Finally, when BITMAP information is enrolled into the three U.S. Government databases (i.e., IDENT, FBI Next Generation Identification, DoD Automated Biometric Identification System), disclaimer language informs the current and future recipient that the enrollment itself does not contain derogatory information and that no action should be taken on the individual solely on the basis of the enrollment.

Privacy Risk: There is a risk that ICE may inadvertently accept BITMAP encounters from foreign partners with human rights violations.

Mitigation: This risk is partially mitigated. ICE does not accept BITMAP submissions based solely on race, ethnicity, national origin, religious affiliation, or First Amendment-protected activities. BITMAP has established various program requirements, training, and oversight mechanisms to safeguard privacy and civil liberties to ensure foreign partner collections are conducted in accordance with the program's purposes and law enforcement objectives.

First, the deployment of a BITMAP initiative in a host country must comply with the program's implementation requirements. Prior to entering an arrangement with a BITMAP foreign partner (whether via formal written agreement or otherwise), the program's BITMAP foreign partner selection process requires that all BITMAP foreign partners undergo a human rights evaluation conducted independently by the Department of State. The Department of State conducts an independent review of proposed BITMAP foreign partners to ensure that there is no history or a known pattern of abuse. The Department of State vetting process evaluates every law enforcement official on the foreign partner's security force. A confirmed human rights violation will exclude that foreign official or foreign partner security force from participating in a BITMAP initiative.

Second, BITMAP foreign partners are required to undergo BITMAP's training program that includes a course objective devoted to the importance of human rights. HSI takes steps to promote best practices and deter civil rights violations through principle-based training and guidance. For example, this training objective includes a review of international norms and standards, such as reaffirming the illegality of racial discrimination. This training objective also includes guidance on human rights standards for the performance of law enforcement duties. For example, BITMAP personnel provide guidance on the proper code of conduct for law enforcement officials based on customary international principles (e.g., use of force, health of individuals while in custody). HSI's training program focuses on educating the foreign law enforcement partner to enable foreign officials to develop skills and apply these standards to their conduct associated with BITMAP operations.

Third, as noted above, BITMAP procedures include a manual review of all enrollments. This manual review is designed to identify and correct (or remove) any encounter errors to include the removal of U.S. citizens, Lawful Permanent Residents, or other Special Protected Class individuals, as appropriate. Foreign law enforcement partners are aware that the biometric collection devices contain a Targeting Selection Criteria that identifies the foreign country originating the BITMAP encounter. The Attaché covering the region inclusive of the foreign partner's jurisdiction maintains situational awareness of country conditions and current events and has routine knowledge of the BITMAP foreign partner's encounters under BITMAP. Program personnel use the Targeting Selection Criteria as an oversight mechanism to monitor BITMAP

encounters for unauthorized activities or abnormal patterns that may deviate from the foreign law enforcement partner's standard encounters and/or that correspond to or are influenced by country conditions and current events. Finally, any confirmed intentional misuse of data may result in the removal of the foreign official from the program and the associated BITMAP encounter(s) or termination of a BITMAP initiative.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

BITMAP enrollments are retained by U.S. Government biometric databases. The retained information is used to assist U.S. domestic and foreign law enforcement officials in furtherance of their official law enforcement activities such as combatting transnational crime and detecting and/or deterring terrorist-related activity. All BITMAP enrollments in U.S. Government databases are retained in accordance with the system's records retention schedule and retention requirements identified in information sharing agreements. ICE is responsible for managing its own records retention requirements for biometric information collected and stored in IDENT. BITMAP enrollments will be stored and retained for 75 years within IDENT and disposed of in accordance with the National Archives and Records Administration (NARA)-approved DHS-wide records retention schedule for biometric records under DAA-0563-2013-0001, or any successor schedule, used for national security, law enforcement, immigration, and other functions consistent with DHS/ICE authorities.[49]

Further, FBI's Next Generation Identification system maintains records about individuals until the individual reaches 110 years of age in accordance with NARA records control schedule N1-065-10-16.[50] DHS data in DoD's Automated Biometric Identification System will be retained consistent with DoD's NARA-approved retention schedule regarding biometrics (DAA-AU-2013-0007), which is 75 years after the cutoff date for the records or when no longer needed for military

[49] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, 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.
[50] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, U.S. DEPARTMENT OF JUSTICE, INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS) AND RELATED RECORDS (2010), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-016_sf115.pdf.

operations or DoD business functions, whichever is later. In either case, ICE can request that specific records be removed from FBI Next Generation Identification or DoD Automated Biometric Identification System if they are no longer needed for BITMAP purposes.

Privacy Risk: There is a risk that BITMAP collects more information than is necessary for the purposes of the program.

Mitigation: This risk is partially mitigated. As noted above, ICE HSI established BITMAP to promote and strengthen the international cooperation and coordination of law enforcement agencies' efforts to combat transnational criminal activity, identify threats of potential terrorism, enhance border security, and enforce customs and immigration laws. BITMAP Advisors train foreign law enforcement partners on these law enforcement objectives to ensure that foreign partners' purposes for collection are limited to criminal activity that aligns with HSI's legal authorities.

In addition, HSI trains and equips foreign law enforcement partners with biometric devices that are compatible with the program's investigative purpose. The program requirements, technical specifications of the devices, and manual review of U.S. Government holdings inherently limit the ability of foreign law enforcement partners to collect large volumes of information from individuals who do not fall within the program's Targeting Selection Criteria. The Targeting Selection Criteria identifies four categories of individuals and purposes for collection. BITMAP foreign partners collect individuals' biometric information to best identify each individual associated with the Targeting Selection Criteria categories and selects the appropriate category.

While fingerprints are automatically searched and compared (and are used as the primary biometric identifier), the other biometric modalities (e.g., palm print, photograph, iris image) are retained for manual verification purposes if a match cannot be made by fingerprints alone. Some BITMAP encounters may not match to U.S. Government holdings. Non-matching enrollments—also known as historical enrollments—submitted under BITMAP may be used to help piece together data points which have been connected to previous (or ongoing) investigations and criminal activities. However, information gleaned from this sharing is used to prevent, detect, and investigate crime, including assessing whether an individual is involved in transnational crime, presents a criminal or terrorist risk, and aids border and immigration-related decisions. These historical enrollments are vital to assisting all international partners to combating current and future transnational criminal activity both now and in the future. BITMAP also collects photographs. A BITMAP enrollment includes taking a frontal facial photo (headshot). The headshot is stored in IDENT and may be used for subsequent facial matching. This is a crucial element of identification.

Privacy Risk: There is a risk that the program collects information on individuals whose information should not be in the system or that have no nexus to the United States.

Mitigation: This risk is partially mitigated. BITMAP collects biographic and biometric information from foreign nationals involved in or reasonably suspected to be involved in transnational and criminal or terrorism-related activity. These individuals' activities pose a threat to the international community, including the United States, regardless of the foreign jurisdiction in which they are operating or plans to travel within or to a jurisdiction harmed by their criminal activities. Therefore, at the point of collection, the foreign partners do not know whether these individuals have or may travel to the United States, only that the foreign national's criminal activity is related to a transnational common interest and international nexus that poses an immigration, criminal, and/or national security risk to the United States and its foreign partners.

Further, in accordance with the mutual understanding struck between HSI and the foreign partners (whether via formal written agreement or otherwise), foreign partners shall focus their BITMAP collections on individuals suspected of participating or facilitating terrorism, transnational organized crime, and other serious crimes. This BITMAP information enables DHS to maintain information about foreign nationals currently posing a threat to the United States and its foreign partners and to identify and prevent or mitigate potential threats.

As discussed above, foreign law enforcement partners transmit BITMAP encounters based on the program's Targeting Selection Criteria and in accordance with the laws, regulations, and policies of their respective jurisdictions. Foreign law enforcement partners collect information from suspect individuals while in custody or during law enforcement investigations and operations when there is an investigative interest that aligns with ICE law enforcement priorities and mission operations. For example, not all criminal offenses would qualify for collection under BITMAP, as certain types of crimes (e.g., burglary) have no transnational interest and fall solely within the foreign partner's local jurisdiction. The intended collection is designed to ensure the foreign partner has access to accurate and complete information of investigative value on a national or international security level.

Agreements with partners focus collections on terrorism, transnational organized crime, and other serious crime that could adversely impact U.S. security. The Attaché reviews the Targeting Selection Criteria and circumstances under which suspect individuals should be targeted during the training program. The Attachés and BITMAP advisors help maintain program integrity with the foreign partners to include reviewing program requirements, guidelines, and enrollment standards. In addition, the Targeting Selection Criteria enable HSI to conduct oversight to ensure the BITMAP encounters are compatible with the program's purpose for collection. The foreign

law enforcement partner's investigative and/or operational encounter information must support the relevant Targeting Selection Criteria. For example, the foreign partner may include derogatory information collected during its investigation, such as a previous gang-related criminal offense and biographic information that affirms the subject's affiliation with a gang (e.g., a tattoo that identifies rank). The Targeting Selection Criteria uses a corresponding country code to identify which foreign partner submitted the BITMAP enrollment.

Finally, BITMAP has established technical safeguards to maintain oversight and enforce program requirements that prevent the automatic retention of U.S. person data in U.S. Government biometric databases in cases where there is no legitimate law enforcement purpose for the collection. As discussed above, the Targeting Selection Criteria require BITMAP foreign partners to use the codes to identify U.S. persons (i.e., Vetting enrollment) submitted under BITMAP. The Vetting category initiates an automatic *search-only* transaction for a U.S. person BITMAP encounter. The U.S. person's encounter is compared with existing information in U.S. Government databases, and the results are provided to the Attaché to determine whether there is an investigative need for its retention. While the BITMAP analyst team will be alerted to the existing record, the Vetting category prevents automatic retention into U.S. Government databases.

If the foreign law enforcement partner does not use the Vetting category to identify the encounter as a U.S. person (possibly because the individual provided fraudulent identity documents), that encounter will be retained in U.S. Government databases for future matches. However, BITMAP encounters are automatically compared against existing identities in U.S. Government databases for deconfliction. The BITMAP analyst team is notified when a foreign partner encounter is found to be a U.S. person subsequent to collection and are required to conduct a manual review of the BITMAP encounter to determine if retention is warranted.

Therefore, where the foreign law enforcement partner assigns an incorrect Targeting Selection Criteria to a U.S. person or where an individual fails to identify themselves as a U.S. person, and there is no legitimate law enforcement purpose to retain the encounter, HSI personnel will contact the corresponding system owner(s) to request the U.S. person's BITMAP encounter be removed from U.S. Government databases. Finally, for U.S. persons who believe their biometrics were collected as the result of an improper BITMAP encounter, DHS provides a redress process (identified above in "Individual Participation" section above).

Privacy Risk: There is a risk that BITMAP enrollments are retained by U.S. Government databases longer than is necessary to fulfill the purposes of the program.

Mitigation: This risk is partially mitigated. As indicated above, the IDENT system retains encounters for 75 years in accordance with the NARA-approved records retention schedule.

Neither DHS nor ICE have control over the retention periods for either the FBI Next Generation Identification system or the DoD Automated Biometric Identification System. Both of those agencies will retain BITMAP enrollments in accordance with their respective NARA-approved records retention schedules. For FBI Next Generation Identification, NARA has approved the destruction of fingerprints and associated information when subjects attain 110 years of age or seven years after notification of death with biometric confirmation. Biometrics such as photographs may be removed from FBI Next Generation Identification earlier than the standard NARA retention period by the submitting agency's request or a court order. For the DoD Automated Biometric Identification System, records are maintained for 75 years, at which point they are deleted and destroyed. ICE may request that either FBI Next Generation Identification or DoD Automated Biometric Identification System delete these records prior to the scheduled destruction if no longer needed for business purposes. For example, when ICE requests that a U.S. person encounter retained in DoD's Automated Biometric Identification System or FBI's Next Generation Identification to be removed.

In addition, BITMAP enrollments may be retained in accordance with the retention requirements outlined in specific information sharing agreements.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

BITMAP discloses information to: 1) assist DHS Components and BITMAP foreign partners in assessing whether an individual presents a criminal or terrorist risk, and to develop leads in furtherance of law enforcement investigations; 2) aid DHS Components and BITMAP foreign partners in law enforcement actions and counterterrorism operations; and 3) aid DHS and other federal agencies in making decisions for national security, law enforcement, counterterrorism, immigration, intelligence, and other functions that require the use of biometric and biographic information, such as preserving the integrity of the immigration systems, disrupting and dismantling Transnational Criminal Organizations and other criminal networks, and identifying and preventing terrorist and criminal threats that risk the safety of U.S. persons and foreign partners. These specified purposes are documented throughout this Privacy Impact Assessment, identified in the program's Targeting Selection Criteria, and used by BITMAP foreign partners in accordance with informal mutual understandings, and documented in negotiated agreements or arrangements. Additionally, the sharing of information is done in accordance with all other federal, state, or local laws, regulations, and policies and is in alignment

with applicable agreements with U.S. Government partners and routine uses detailed in the related System of Records Notices.

Privacy Risk: There is a risk that data will be shared with external parties who do not have a need to know.

Mitigation: This risk is partially mitigated. ICE shares information to authorized third parties who have a need to know the information, and only for uses that are consistent with the stated purposes for which the information was originally collected. HSI is responsible for all BITMAP encounters enrolled and stored in the DHS-wide biometric database, IDENT. The sharing of BITMAP information maintained in IDENT with other U.S. Government agencies occurs in accordance with departmental policies and information sharing agreements (e.g., Memorandum of Understanding, Memorandum of Agreement) with DoD and FBI. These agreements identify authorized users who receive access to the system and set forth the terms and conditions for sharing DHS information. These agreements also contain provisions requiring concurrence among the U.S. Government agencies before the recipient can share information with a third party.

Only authorized HSI personnel of U.S. Government databases have access to BITMAP encounter information and any other sensitive information (e.g., intelligence, personally identifiable information returned as the result of a match. HSI personnel will determine whether there is investigative value in the derogatory information (e.g., criminal history, warrants, International Criminal Police Organization notices) and legal authority to facilitate and coordinate the sharing of information with other U.S. domestic and foreign partners in accordance with agency-related mission functions.

In addition, HSI has established privacy safeguards to control and prevent the unauthorized and inadvertent sharing of DHS information. HSI maintains technical access controls to ensure the sharing of BITMAP information adheres to departmental policies and information sharing agreements. HSI manually controls the sharing of information maintained in DHS systems. BITMAP foreign partners *do not* have access to U.S. Government databases, or any law enforcement information or other sensitive information maintained that may be returned as the result of a BITMAP encounter.

BITMAP foreign partners may contact the Attaché when notified of a match. The Attaché will share any relevant information with the foreign partner on a case-by-case basis. The Attaché conducts a review of the information associated with a BITMAP match and determines whether there is any potential investigative value of sharing that information with the BITMAP foreign partner. Any information shared with the foreign partner is shared in accordance with all laws and

regulations and complies with approved policies and guidelines at the Attaché post, including the ICE Directive on the "*Safeguarding Law Enforcement Sensitive Information*"[51] and DHS Privacy Policy.

Additionally, DHS policy pertaining to the use and sharing of personally identifiable information may also be reflected in applicable agreements, arrangements, and other implementing documentation. For example, these agreements and arrangements define the purpose and scope for which the information can be used, limit onward sharing, and require partners to ensure the data is secured and safeguarded.

As noted above, traditionally ICE and BITMAP foreign partners have simply established a common or mutual understanding for BITMAP information sharing and exchange. ICE has recently developed an information sharing template to memorialize the BITMAP information sharing practice. The ICE Directive on the "*Development and Approval of Information Sharing Access Agreements*" will inform the development of information sharing instruments with foreign partners.[52] Among other requirements, the information sharing agreements will document and provide notice to the BITMAP foreign partner on how its information will be used and shared with U.S. Government partners and the limitations on the use and sharing of U.S. information shared with the BITMAP foreign partner.[53]

These administrative and technical privacy safeguards allow BITMAP to adhere to program requirements and maintain program oversight to ensure information is shared in accordance with ICE legal authorities, BITMAP functions, departmental policies, and information sharing agreements.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

ICE ensures the quality and integrity of its data in several ways. First, ICE BITMAP personnel train the foreign partners to identify individuals who meet one of the Targeting Selection Criteria described above. The training also instructs foreign partner personnel on the appropriate use of the biometric collection devices, which requires the foreign partner to select one of the

[51] *See* ICE Directive 4003.2 "*Safeguarding Law Enforcement Sensitive Information*," (May 20, 2014).
[52] For foreign partners which are European Union member states, the European Union-U.S. information sharing framework Data Protection and Privacy Agreement (DPPA) will also be followed when developing and memorializing information sharing practices.
[53] *See* ICE Directive 4006.1 "*Development and Approval of Information Sharing Access Agreements*," (Nov. 24, 2020).

corresponding codes associated with one of the categories of individuals identified in the Targeting Selection Criteria in order to submit a BITMAP enrollment. The Attachés conduct regular reviews and audits of the information entered into U.S. Government databases to mitigate the risk of data inaccuracy and ensure that the information maintained by IDENT, FBI Next Generation Identification, and DoD Automated Biometric Information System is as accurate, complete, and relevant as possible.

Second, an ICE BITMAP analyst conducts a manual review of each BITMAP encounter for data quality and integrity purposes. If the analyst discovers that an encounter pertains to either a U.S. person or a member of a Special Protected Class, that data is purged from the U.S. Government databases and will not be used for matching purposes, unless there is a legitimate law enforcement purpose for retention. The ICE BITMAP analyst looks at each BITMAP encounter to confirm that the foreign partner selected the appropriate code based on the individual whose biometrics were collected.

Privacy Risk: There is a risk that the U.S. Government databases could contain inaccurate information about individuals, and that ICE may take adverse action based on this information.

Mitigation: This risk is partially mitigated. First, BITMAP adheres to the standards set forth by the National Institute of Standards and Technology (NIST), which advocates collecting fingerprints to improve the accuracy of identifying individuals.[54] BITMAP biometric collection devices employ ten-print matching, which is automatically compared to the best quality biometrics associated with each identity in the IDENT system. Identification with all ten fingerprints enables more accurate and comprehensive searches against other U.S. Government biometric databases. Ten-print matching also improves the quality of data associated with an individual and decreases the chance of false negative and false positive matches.

Second, BITMAP equips foreign law enforcement partners with biometric collection devices that are compatible with DHS and other U.S. Government biometric databases to safeguard data quality and the integrity of biometrics. The biometric collection devices have built-in algorithms that perform quality checks to guarantee that the quality of fingerprints captured meets acceptable standards and is sufficient for enrollment into U.S. Government systems. In addition, IDENT performs certain quality checks (e.g., determining the quality of a captured fingerprint and

[54] *See* Testimony of Dr. Martin Herman, Chief, Information Access Division, Information Technology Laboratory, National Institute of Standards and Technology before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Ensuring the Security of America's Borders through the Use of Biometric Passports and other Identity Documents (Jun. 22, 2005).

its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness.[55]

Third, the Attaché and BITMAP Advisors train foreign partners on how to use the biometric collection devices to ensure BITMAP encounters are complete and transmissions are successful. A complete BITMAP encounter identifies the BITMAP foreign partner that transmitted the encounter, biometric and associated biographic data, and the category of encounter (i.e., International and National Security, Person of Interest, Gang Member, Vetting). This information is collected by the foreign partner directly from the individual, increasing the likelihood that the biometric and biographic data captured is accurate.

Fourth, HSI personnel routinely review BITMAP encounters to ensure foreign law enforcement partners provide a complete BITMAP encounter. Foreign law enforcement partners collect biographic information from individuals involved in criminal or law enforcement-related activity and thus, the individual may provide incorrect information to mislead the foreign partner's investigation or to avoid detection. For example, the criminal suspect involved in illicit activity may provide fraudulent identity documents to prevent authorities from discovering their identity and association with other criminal activities, networks, or to avoid extradition. Therefore, the information is as accurate as the statements and documentation that the individual provides. However, it should be noted that even if the individual provides the foreign partner with false biographic information, U.S. Government databases determine the existence of a "match" based on the biometric data, providing a significantly higher degree of accuracy. Thus, the use of biometrics helps ensure accuracy of identification.

Finally, HSI personnel manually review information maintained in other DHS systems before sharing information or taking any enforcement action. Checking the availability of new or updated subject records in the system(s) for purposes of deconfliction ensures that all users have the most complete and accurate information available at any given time. All ICE employees are trained in areas such as data quality and integrity, to confirm the accuracy, completeness, and quality of the information. HSI program personnel use other investigative techniques, sources, and leads to verify and corroborate the accuracy of the information and do not solely rely on BITMAP encounters to take adverse action against any individual. HSI BITMAP personnel will review each encounter to confirm that the correct Targeting Selection Criteria was used at the point of collection and that encounters pertaining to U.S. persons or Special Protected Classes are purged

[55] As additional biometric modalities become available for use through this program, DHS will analyze the privacy implications of those modalities and develop policies and procedures, if necessary, to mitigate potential privacy risks related to data quality and integrity. Any new developments will be addressed in an update to this Privacy Impact Assessment.

from U.S. Government databases. HSI BITMAP personnel also manually review all nominations to the Terrorist Screening Database to determine suitability.[56] The sole existence of a BITMAP encounter is not sufficient for eligibility to the Terrorist Screening Database, and no information is automatically pushed into the Terrorist Identities Datamart Environment.[57] Individuals also have mechanisms to access and amend any records maintained by the U.S. Government, and ICE will correct any records determined to be inaccurate, as appropriate under policy and law. More information about the access and amendment process can be found above in the Fair Information Practice Principles section, "Individual Participation."

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

BITMAP information enrolled and maintained in IDENT is shared internally within DHS and the U.S. Government databases identified above (i.e., FBI Next Generation Identification, DoD Automated Biometric Information System). Only authorized users with a need to know have access to U.S. Government databases and the sensitive personally identifiable information contained within. In addition, system administrators employ role-based access controls to ensure only authorized users can access information in a system that is necessary to perform their official duties. Any suspected or confirmed misuse of data, unauthorized access to a database, or inappropriate disclosure of sensitive information must be reported and handled as a privacy incident. For cases of potential misuse of data by ICE personnel, the incident will be reported to the ICE Office of Professional Responsibility (OPR) for further investigation.

Neither the BITMAP Advisors nor the Attaché share any U.S. Government information with the foreign law enforcement partner(s) based solely on a match to a record within one of the U.S. databases. The Attaché receives any U.S. Government information developed as a result of a BITMAP encounter and that may be appropriate for sharing with a foreign partner; the Attaché reviews the information and shares only that which is relevant and necessary for investigative purposes in accordance with program requirements. Should foreign partners seek additional information, they must contact the Attaché in writing.

---

[56] The Terrorist Screening Database is owned by the FBI's Threat Screening Center (TSC). For more information about the Terrorist Screening Database, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE WATCHLIST SERVICE, DHS/ALL/PIA-027 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[57] For more information about the Terrorist Identities Datamart Environment, *see* https://www.dni.gov/files/NCTC/documents/features_documents/TIDEfactsheet10FEB2017.pdf.

Finally, HSI has established strict security and privacy access controls for BITMAP to safeguard against unauthorized access or inappropriate disclosure of sensitive information, including information pertaining to U.S. persons or members of Special Protected Classes, as these protected individuals are afforded additional confidentiality protections by statute. ICE requires that any system maintaining such information establish a mechanism for identifying individuals who are protected by confidentiality laws or policies.[58]

Privacy Risk: There is a risk that the program does not protect against unauthorized access, use, destruction, or modification of information.

Mitigation: This risk is partially mitigated. BITMAP has implemented technical access controls to safeguard information both in transit and when received and maintained in DHS systems. BITMAP provides foreign law enforcement partners with biometric collection devices which only retain individual encounter and enrollment data locally, on the device itself, and that have no ability to access U.S. databases. As a further mitigation, devices purchased after 2022 may be remotely wiped of data by HSI personnel. HSI BITMAP personnel also train foreign law enforcement partners on how to securely transmit information using a DHS encrypted one-way portal. This security measure mitigates the risk that data on BITMAP encounters will be compromised during transmission.

As discussed above, BITMAP foreign partners do not have access to U.S. Government databases, thereby preventing unauthorized users from accessing or using law enforcement and/or other sensitive information (e.g., personally identifiable information). Program requirements restricting the foreign law enforcement partners' automated access to BITMAP encounter responses helps further mitigate the risk that foreign partners will access sensitive information or share such information without first receiving approval from ICE. As discussed above, the only information that ICE automatically sends back to the foreign partner is a notification of a successful enrollment and, in certain situations discussed above, for the foreign partner to contact their BITMAP Advisor for further information. Foreign partners must contact their BITMAP Advisor to request specific information regarding individual enrollments.

Finally, HSI BITMAP personnel conduct a manual review of all BITMAP encounters and will remove any records pertaining to U.S. persons or members of Special Protected Classes whose information should not be retained in U.S. Government databases or otherwise shared with foreign

[58] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY DIRECTIVE 002-02, REV. 00.1, IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS (Apr. 29, 2019); U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY INSTRUCTION 002-02-001, IMPLEMENTATION OF SECTION 1367 INFORMATION PROVISIONS (Nov. 7, 2013), on file at the DHS Privacy Office.

partners. This manual review process further enhances the security of the data.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

U.S. Government agencies which maintain BITMAP information employ multiple mechanisms to audit the use of personally identifiable information and ensure that such use is compatible with the Fair Information Practice Principles and complies with all applicable privacy laws, regulations, and policies. First, HSI BITMAP personnel extensively train the Attachés and BITMAP Advisors (who in turn train the foreign partners) regarding program specifics, the appropriate use of the biometric collection devices, using the Targeting Selection Criteria, and human rights concerns. Additionally, authorized users of U.S. Government databases complete mandatory privacy training and system-specific, role-based training regarding the collection, use, maintenance, and sharing of personally identifiable information in the applicable databases (i.e., CBP Unified Passenger system, IDENT, FBI Next Generation Identification, DoD Automated Biometric Information System).

Second, the Attachés or the BITMAP analysts review BITMAP encounters to confirm that any BITMAP information maintained in U.S. Government databases meets BITMAP's Targeting Selection Criteria and the program's law enforcement objectives. If the Attaché determines that foreign partners are collecting information from individuals whose information does not meet the program's requirements, then that enrollment would be removed from U.S. Government databases.

Finally, ICE is implementing a training requirement requiring the foreign partners to attend a biannual refresher training. This refresher training will include updates on device use, requirements for enrollment/targeting criteria, and adherence to applicable agreements. The Attachés will support this training as part of their role in the information sharing process.

Privacy Risk: There is a risk that BITMAP encounters are not audited or accounted for in a manner consistent with Privacy Act requirements and DHS policy.

Mitigation: This risk is partially mitigated. As indicated above, ICE has implemented a robust training program for the Attachés and BITMAP Advisors, who in turn provide training to foreign partners. In addition, HSI BITMAP personnel's manual reviews of BITMAP encounters guard against the ingestion of U.S. persons' information without specific, articulable law enforcement purpose. Further, records shared with DHS foreign partners in response to a BITMAP encounter are done within the Title 19 Law Enforcement Information Sharing guidelines, when

made part of a report of investigation (ROI) they tracked and recorded either in the corresponding source system or other ICE system of records. In accordance with the Privacy Act and DHS policy, disclosure of records is accounted for through, for example, documentation within the relevant ICE systems of records or local documentation procedures established by Attachés. Records shared with foreign partners can be identified through a review of the documented disclosure and can be audited as necessary. In some situations, primarily related to national security, other federal agencies may assume the lead investigative response to a BITMAP encounter, to include direct communication with the foreign partner. In those cases, the relevant federal agency would follow its own governing processes to account for any further information disclosure.

ICE also relies on OBIM to retain an accounting of biometric records disclosed outside of DHS. The disclosures include paper-based or electronic records and document the date, nature, and purpose of each 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 applicable systems to re-create the information to demonstrate compliance. BITMAP enrollments with matches to records from IDENT, FBI Next Generation Identification, and/or DoD Automated Biometric Information System are retained in a hot list, which can be used for auditing purposes.

Additionally, applicable DHS systems (i.e., CBP Unified Passenger system, IDENT) maintain audit records for any information shared with an external agency, as described in their respective Privacy Impact Assessments. For example, audit logs are maintained by the IDENT Operations and Maintenance Team and the Information Technology Management Branch. Access to audit logs is limited strictly to core IDENT Operations and Maintenance personnel. The audit log data is backed up regularly as part of the overall IDENT database backup and archiving process. Finally, BITMAP personnel use the Targeting Selection Criteria as an oversight mechanism to audit the data collection process to ensure foreign law enforcement partners comply with the program's requirements. For example, the Targeting Selection Criteria allows program personnel to track BITMAP encounters back to the foreign partner who submitted the information. The HSI Attachés are assigned to U.S. Embassies or Consulates in foreign countries and, therefore, are able to work closely with the foreign partner to monitor BITMAP encounters to identify unauthorized activities or abnormal patterns of collection.

As noted above, BITMAP has established protocols in place if the BITMAP foreign partner submits enrollments that are not in compliance with the program's law enforcement objectives. Any improper BITMAP encounter may be removed unless there is a legitimate law enforcement purpose to retain the record. When that happens, HSI contacts all internal and external government partners to remove the individual's biometric record from their respective systems. Finally, the

intentional misuse of the biometric collection devices, such as BITMAP encounters based on race or national origin, will result in the removal of the foreign official from the program or the possible termination of BITMAP with the foreign partner.

Further, the DHS Privacy Office will begin its own audit, with assistance from ICE, within 90 days of the approval of this Privacy Impact Assessment to ensure that the requirements and processes outlined herein are being followed. The DHS Privacy Office, at its discretion, may determine a follow-up review or additional auditing mechanism is necessary. Should any significant programmatic changes be necessary based on the findings of that audit, this Privacy Impact Assessment will be updated.

Responsible Officials

Ricardo Mayoral
Assistant Director, Homeland Security Investigations/International Operations
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Kenneth N. Clark, Ph.D.
Assistant Director, Management and Administration/
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

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

_____

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov