HOMELAND SECURITY ADVISORY COUNCIL

Final Report of the Biometrics Subcommittee

November 12, 2020

This page is intentionally left blank.

This publication is presented to the Honorable Chad F. Wolf, Acting Secretary of the Department of Homeland Security (DHS) on behalf of the Homeland Security Advisory Council (HSAC), Subcommittee on Biometrics. The Biometrics Subcommittee is led by Judge Robert C. Bonner (Chair) and Leon Fresco (Vice Chair).

<SIGNATURE OBTAINED FOR PDF COPY>

Robert C. Bonner

Principal, Bonner ADR & Consulting Services

Leon Fresco

Partner, Holland and Knight

This page is intentionally left blank.

Subcommittee on Biometrics

Robert C. Bonner (Chair)	**Principal, Bonner ADR & Consulting Services**
Leon Fresco (Vice Chair)	**Partner, Holland and Knight**
Jayson Ahern	**Principal and Head of Security Services, The Chertoff Group**
Michael P. Jackson	**President and Founder, Firebreak Partners, LLC**
Hans Miller	**CEO, Airside Mobile, Inc.**
Chad Sweet	**Co-Founder, The Chertoff Group**
Karen Tandy	**Administrator (Retired), Drug Enforcement Administration**

Homeland Security Advisory Council Staff

Michael Miron, Acting Executive Director, HSAC

Garret Conover, Director, HSAC

Evan Hughes, Associate Director, HSAC

Colleen Silva, Analyst, HSAC

Table of Contents

Executive Summary

Since its inception in early 2003, operational agencies of the Department of Homeland Security (DHS) have made innovative and effective use of biometrics. From US-VISIT to Global Entry, the integration of biometrics to better protect the U.S. homeland and improve performance of the diverse missions of DHS has been impressive. However, when DHS was stood up in 2003, some biometric tools, such as facial recognition and iris scans, were in their infancy or nonexistent altogether.

In recent years, the use of biometrics by some DHS components, particularly facial recognition, has caused controversy and called into question whether the Department's processes and procedures for vetting and adopting new uses of biometrics are adequate. Moreover, in the absence of an overarching department-wide process, there is concern that DHS has missed opportunities to leverage the biometric innovations of one DHS component to other components with similar missions. Further, in some situations, *e.g.*, the rollout by U.S. Customs and Border Protection (CBP) of biometric exit in 2018, departmental level buy-in was lacking, and there was not a comprehensive communication and outreach strategy prior to implementation.

Having studied how DHS agencies are currently using biometrics and DHS's existing coordination and oversight mechanisms – and giving due consideration to the organizational structure of DHS -- we conclude the Department would benefit by developing a coordinated oversight and vetting process regarding the use of biometric tools, with a key focus on any proposed uses of new biometrics and novel uses of existing biometrics. The oversight and coordination council that we envision would be chaired by the Deputy Secretary and involve representation of all DHS operational agencies, as well as relevant departmental-level support offices. In order to ensure that privacy considerations are recognized and appropriately considered, the DHS offices of Privacy and Civil Rights and Civil Liberties would have chairs on this council.

The Subcommittee recommends that any DHS operational agency seeking to implement a material change to a currently approved biometric tool or to implement a use of a new biometric tool must submit to a Biometrics Oversight and Coordination Council (Council) a formal implementation plan. Such proposals would clearly explain the plan of action and its implementation. Each such proposal should also include a separate communication outreach plan, covering both internal DHS coordination and appropriate external outreach. After appropriate review and recommendations by the Council, the Deputy Secretary would accept, reject or modify the proposal.

We also are mindful of the need for nimbleness and flexibility in this area of evolving technology. Indeed, without such agility, it is doubtful that many of DHS's most innovative and effective uses of biometrics would have occurred. In other words, while we recommend a new structural review process for biometrics, we do not wish to crush innovation by establishing new or arduous bureaucratic hoops. To that end, our recommendations recognize the need for a fast-track process to permit rapid approval of pilot projects in order to evaluate how and whether biometrics can be effectively implemented into a DHS agency's operational protocols. This fast-track process is also essential to quickly address emerging threats, such as rapid approval for DNA testing in light of false claims of parentage and recycling of tender-aged children that occurred during last year's family unit migration crisis.

Key Recommendations[1]

To that end, we briefly summarize our key Recommendations:

- DHS should establish a Biometrics Oversight and Coordination Council (BOCC), with representation by the appropriate DHS component agencies and offices. The BOCC would be chaired by the DHS Deputy Secretary and would, among other things, review both implementation and communication plans submitted by a proposing DHS operational agency. (Recommendations 1 and 8).
- The operational role for the collection and uses of biometrics should remain with the DHS agency that has the unique mission or program that is aided and/or made more effective with the use of biometrics. That agency has the responsibility for submitting an implementation plan for any new use of biometrics to the BOCC. (Recommendations 4 and 9).
- Every new use of a biometric should require, in addition to an implementation plan, the preparation and submission of a separate communication/outreach plan. (Recommendation 8).
- In an effort to improve and encourage agility, the BOCC protocols should provide a fast-track process to approve pilots and emergency uses of biometrics, to include direct interaction between the Deputy Secretary, as Chair of the Council, and the relevant agency head. (Recommendation 2).
- Where sharing of biometrics involves negotiations with other nations, the DHS Office of Policy should have the lead role, but the operational component(s) with equities and established relationships should play an active role in the negotiations. (Recommendation 7).

[1] A complete set of the Subcommittee's Recommendations can be found in section IX of this Report.

I. Introduction

a. The Tasking and Formation of the HSAC Subcommittee

By letter dated February 21, 2020, Acting Secretary of Homeland Security Chad F. Wolf requested that the Homeland Security Advisory Council (HSAC)[2] convene a Subcommittee to examine the need for and how the Department can better develop and implement a single and reliable approach to biometric identity management.

The tasking requested recommendations from the Subcommittee relating to seven areas, to include: (1) how the Department of Homeland Security (DHS) can establish a multi-year biometrics vision, strategy and implementation plan with performance metrics and oversight; (2) how it can establish clear roles and responsibilities within and between Department Components and Offices regarding the collection and use of biometrics; (3) best practices, if any, to create a biometric enterprise and governance process; (4) how DHS can establish consistency regarding how it shares biometrics with other federal, state, local, tribal and international law enforcement/security partners and with the private sector; (5) how DHS can better communicate with the public, Congress and stakeholders about how it intends to use and protect biometric information regarding new uses of biometrics and novel uses of existing biometric modalities; (6) how DHS can improve its biometric collection, storage, matching, analysis and sharing capabilities, including uses of new and emerging biometric modalities to support DHS missions; and (7) provide insight into how DHS can create a systematic and fully functioning Planning, Programming, Budgeting, and Execution (PPBE) process for biometrics. See Appendix 1.

As is evident, the taskings are primarily about process, and *not* about evaluating how specific biometric tools can be used more effectively, nor which biometric modality is best fit for specific DHS missions. Indeed, the Subcommittee was not tasked with evaluating the policy merits of specific biometric modalities and has not done so.

Pursuant to the Secretary's taskings, the Subcommittee undertook to review: (1) how DHS operating agencies and its relevant administrative support entities are currently using biometrics – and for what purposes; (2) the Department's vision and strategy for use of biometrics, (3) how biometrics are or should be shared inside and outside of DHS; and (4) how to ensure that biometric data gathered or used is appropriately collected and protected.

To carry out its charge, the Subcommittee evaluated the need for an overarching department-wide policy regarding use of biometrics and how such an overall department policy is best developed and coordinated within DHS. We also assessed existing departmental-level coordinating mechanisms relating to biometric use, data sharing and protection. We considered how data collection, sharing and protection could be improved. In addition, we analyzed the roles and responsibilities within and between Department headquarters offices and its component agencies for various purposes relating to

[2] A glossary of acronyms can be found at Appendix 6.

biometrics. Finally, based on our extensive review, the Subcommittee developed a set of ten (10) recommendations related to the taskings. *See* Section IX below.

b. The Subcommittee's Process

The members of the Subcommittee of the HSAC, including the Chair and Vice Chair, were appointed in March 2020. In order to gather the necessary background information to understand and respond to the taskings, the HSAC Biometrics Subcommittee held seven meetings, all of which have been virtual. We heard from 31 subject matter experts[3] and reviewed hundreds of documents regarding how DHS and its components collect, use, store, protect and share biometric data – both internally and externally. We interviewed representatives from all DHS component agencies, except FEMA and CISA,[4] and from the relevant DHS department-level offices, including the offices of Biometrics and Identity Management (OBIM), Policy (PLCY), Privacy (PRIV), Civil Rights and Civil Liberties (CRCL) and Science and Technology (S&T). Although not part of DHS, we also heard from the National Institute of Standards and Technology (NIST). Further, we interviewed Non-Governmental Organizations (NGOs) knowledgeable about the privacy implications regarding the collection and use of biometrics, including representatives of the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC). In addition, we heard from representatives of the airlines industry, Airlines 4 America (A4A) and the International Air Transport Association (IATA).

Our review involved gaining an understanding of the different missions of each of the DHS' operational agencies, including the purposes for which they use biometrics to carry out their diverse missions. The Subcommittee was also briefed on how and when DHS shares biometric data with other federal, state and local agencies and with foreign law enforcement counterparts and issues involving negotiations and management of such sharing agreements. We also examined existing policies, strategies and coordination mechanisms used by the Department bearing on the use of biometrics, to include the Department's Biometrics Strategic Framework (2015-2025); the Biometrics Capabilities Executive Steering Committee (BC-ESC), and the Acting Secretary's delegation, issued on December 9, 2019, which references biometrics.

Although the Subcommittee gained a working knowledge of the different biometric technologies being used by component agencies of the Department, the Subcommittee has not attempted to determine the "best" biometric technology for any particular program or mission of the DHS and its component agencies, as this was outside our taskings and is best addressed by the Department and its operational agencies. As biometric technologies continue to evolve, this is and should be an ongoing process for the Department's headquarters offices and its component agencies that collect and use biometrics.

Even as to current biometric technologies, attempting to develop a single solution is likely a mistake given the significantly different missions of DHS' operational agencies. The agencies of DHS present

---

[3] *See* Appendix 4: Subject Matter Experts.

[4] Unlike the six DHS operational agencies we interviewed, neither CISA nor FEMA collect or use biometrics, except for personnel hiring.

a unique case of "one size doesn't fit all." Any overarching strategy, therefore, should preserve, and indeed enshrine, flexibility and agility within DHS components. Whatever is done to improve overall policy approaches and coordination at the departmental level, care must be taken that they do not stifle innovation at the agency and programmatic level.

The Subcommittee notes that on September 11, 2020, U.S. Citizenship and Immigration Services (USCIS) published a proposed rule for public comment purportedly seeking authorization for certain uses of biometrics by USCIS.[i] Despite the Subcommittees' request that it be provided a copy of any proposed rule relating to biometrics, none were furnished. Indeed, the Subcommittee learned about the pending Notice of Proposed Rulemaking (NPRM) from a news story published a few days prior to the NPRM's publication. The USCIS NPRM is a complex and lengthy, 328-page document. The NPRM's public comment period lasted 30 days after its publication (plus an additional 30 days for some specific parts of the NPRM) and USCIS is presently undertaking a review of the more than 5,000 public comments submitted before a final rule is issued; a process that will likely take many months. Released as a proposed USCIS rule, the authorization put forward in the NPRM also appears to apply to CBP and ICE and possibly other component agencies of the Department.

To be clear, this HSAC Subcommittee was not provided with a copy of the NPRM before it was submitted to the Federal Register for publication. Nor did it have an opportunity to consult with USCIS, other DHS agencies, and non-DHS entities regarding the NPRM's drafting or potential impact.

As a practical matter, at the time that USCIS released its NPRM, the HSAC Biometrics Subcommittee was finalizing this report for submission to the full HSAC for approval and transmission to the DHS Acting Secretary. The Subcommittee has therefore concluded that it would be inappropriate for it to comment on the pending USCIS rulemaking document in our report, and it takes no position regarding the substantive merits of the proposed rule.

II. How DHS Agencies Use Biometrics

a. Background

Biometrics are collected and used by DHS' operational agencies primarily to verify the identity of individuals with whom DHS component agencies interact while carrying out their diverse missions. There are several biometric modalities available including, but not limited to, fingerprints/finger scans (FP)[5], facial recognition (FR), iris, voice, and Deoxyribonucleic Acid (DNA). As discussed below, while some DHS component agencies are using FR and DNA in limited ways, overwhelmingly the biometric primarily collected and used by the DHS is FP; a mainstay biometric that began being collected by the Federal Bureau of Investigation (FBI) nearly a century ago.[6] Indeed, "…fingerprint-based biometric systems are so popular and successful that they have become synonymous with the notion of biometric recognition in the minds of the general public."[ii] Thus, all DHS law enforcement component agencies collect and use FP for traditional law enforcement purposes relating to investigations, arrests for federal crimes, and arrests of wanted individuals pursuant to state warrants.

There are eight component agencies of DHS. Six of them - - U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), Immigration and Customs Enforcement (ICE), United States Secret Service (USSS), and U.S. Citizenship and Immigration Services (USCIS) - - are operational agencies that collect and use biometrics. As mentioned earlier, two components, Federal Emergency Management Agency (FEMA)[7] and the Cybersecurity & Infrastructure Agency (CISA), do not collect or use biometrics, except for hiring.

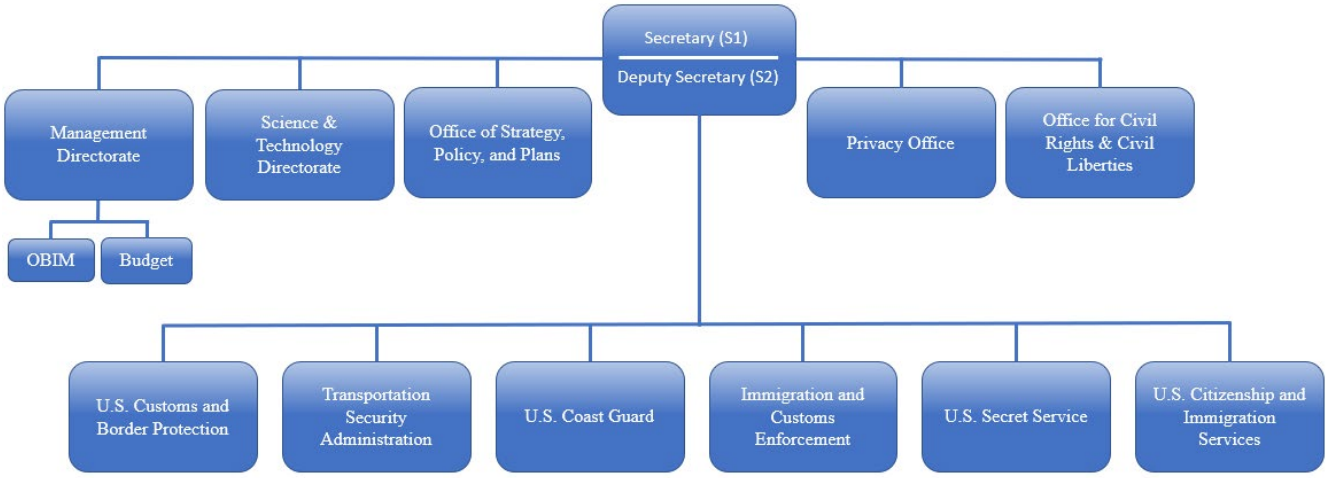
---

[5] We use "fingerprints", "finger scans", and "FP" interchangeably throughout this report. Almost all "fingerprints" collected by DHS agencies are scans/photos of the unique patterns and ridges of the tips of the fingers. Since the invention of finger scan devices, actual "inked" fingerprints have become a thing of the past.

[6] Since 1924 when it began collecting fingerprints from arrestees as part of the booking process, the FBI has been responsible for the national repository of fingerprints and related criminal history data, primarily for persons arrested for crimes by federal, state and local law enforcement agencies. This is when, for investigative purposes, the FBI lab began matching unknown or latent prints from crime scenes with known prints of persons with prior arrests or convictions.

[7] FEMA is considering the use of biometrics to help verify the identity of disaster relief claimants.

DHS Simplified Organizational Chart



Current November 2020

[Figure 1: *DHS Organization Chart showing only the component agencies and departmental offices that play a significant role in the collection, use, storage and policies surrounding biometrics*.]

Five DHS component agencies – CBP, ICE, USSS, USCG, and TSA[8] – are law enforcement agencies (LEAs), that is, they have trained law enforcement officers (LEOs) who are empowered to investigate and/or arrest individuals for violations of federal law or pursuant to warrants for arrest for violations of state laws. They also are authorized to conduct searches, pursuant to lawful authority, and seize contraband. At our nation's ports of entry last year (FY2019), in addition to 288,523 foreign nationals denied entry into the U.S., CBP officers arrested 8,546 persons entering the U.S. for smuggling or who were wanted for crimes.[9] Further, CBP officers seized 227.6 tons of illegal drugs. Between the ports of entry, largely proximate to the U.S. border with Mexico, CBP Border Patrol Agents apprehended 859,501 aliens illegally entering the U.S. last year. Of this number, 114,311 were arrested and referred to the U.S. Justice Department for prosecution. CBP's Border Patrol also seized 147 tons of illegal drugs. ICE HSI Special Agents arrested 37,547 individuals for violations of federal law. ICE ERO apprehended 143,099 aliens and carried out the deportation of 267,258 subjects. USCG arrested 611 suspected smugglers, primarily on the high seas, and seized 165.5 tons of illegal drugs, mainly cocaine. USSS carried out 2,282 arrests for violations of federal criminal laws within its jurisdiction.

Like all federal LEAs, persons arrested by DHS law enforcement agencies for crimes are fingerprinted (finger scans) and have a photo taken at time of booking, and the fingerprints of those arrested for

[8] Although TSA screeners are not LEOs, TSA's Federal Air Marshals are LEOs; they are authorized to carry firearms and make arrests.

[9] CBP's lookout list includes those who have outstanding federal and state arrest warrants.

crimes are submitted to the FBI's Next Generation Identification (NGI) system,[10] the world's largest electronic repository of biometric and criminal history information. Collecting and submitting fingerprints of persons arrested for criminal offenses to the FBI has been standard procedure for all federal LEAs and most state and local LEAs going back decades. As colleting biometrics for those arrested for crimes is primarily a DOJ/FBI responsibility, the Subcommittee did not evaluate DOJ's specific responsibilities in a comprehensive manner.

All DHS agencies and some other federal, local and state LEAs separately submit fingerprints to the Office of Biometrics and Identity Management (OBIM), a programmatic office within DHS which manages the Automated Biometric Identification System (IDENT) system. OBIM determines, from fingerprint matches, whether the person has a prior history of violating U.S. immigration laws, *e.g.,* a prior illegal entry, deportation or removal.

b. Historical Perspectives Regarding Uses of Biometrics by DHS

Expansion of IDENT to Permit Criminal History Checks of Persons Apprehended Illegally Entering the U.S.

In 1994, many years prior to the creation of DHS, the Border Patrol, then part of the Immigration and Naturalization Service (INS), developed the IDENT system in order to identify illegal migrants apprehended crossing our border and, as many had no documents and used false identities, determine whether they had been apprehended on previous occasions by the Border Patrol. Initially, the IDENT system used two fingerprints (index fingers). While IDENT was effective in identifying recidivists, it was not sufficient to run through the FBI's fingerprint database, NGI, known then as the National Crime Information Center (NCIC). As a consequence, the Border Patrol lacked visibility into aliens arrested for illegally crossing the U.S. border who were also wanted for or had been convicted of crimes during a previous period of illegal residence in the U.S.

Following the creation of DHS in 2003, CBP, to which the entire Border Patrol was transferred, expanded IDENT to accommodate full 10-print FP submissions. This was accomplished in 2004, which allowed CBP Border Patrol to identify not just recidivists in terms of illegal entry through IDENT, but also those who earlier had committed serious and violent crimes while in the U.S. as reflected in the FBI's NGI. In turn, CBP was able to take appropriate action, including criminal prosecution.[11]

---

[10] Starting in 2011, NGI began to incrementally replace the Integrated Automated Fingerprint Identification System (IAFIS), to provide a platform for multimodal functionality that can evolve with new technological advances to verify identity and to determine if an arrested individual has a prior criminal record. Pursuant to the DNA Identification Act of 1998, the FBI began collecting DNA samples, in addition to fingerprints of arrestees and convicted offenders. As NGI is managed by DOJ/FBI, not DHS, it is outside the purview of the Subcommittee's taskings.

[11] E.g., having such information often allowed CBP Border Patrol to secure criminal prosecution by the U.S. Department of Justice for illegal aliens with a prior criminal record for felony violation of 18 U.S.C. sec. 1326.

Establishing Biometric Entry for Foreign Nationals Arriving at U.S. Ports of Entry

After the 9/11 attacks, and consistent with later recommendations of the 9/11 Commission[iii], DHS stood up the US-VISIT program for the purposes of collecting biometrics in the form of fingerprints and a digitized photograph of all non-U.S. persons[12] seeking to enter the U.S. through the official ports of entry, primarily those arriving to U.S. international airports. This was a novel use of an existing biometric, and the U.S. was the first nation to collect biometrics from foreign nationals on arrival.

The operational agency for implementing US-VISIT was and still is CBP. Starting in 2004, fingerprint biometrics have been collected by CBP on all foreign nationals arriving at U.S. airports. The finger scans are provided to the IDENT system, now housed in OBIM, as well as run against the FBI's NGI for matches. Thus, the recommendation of the 9/11 Commission and the 2002 Congressional mandate for biometric verification on *entry* at our international airports was accomplished over fifteen years ago.

The real-world successes of using biometrics have disrupted criminals and adversaries from getting into the U.S and from carrying out illegal activities in the U.S. and threatening American lives. Since 2004, CBP has successfully identified persons using false identities and been able to arrest individuals who were wanted but were attempting to enter the U.S. under assumed names and/or fraudulent passports. CBP has also run all those fingerprints against the database of known or suspected terrorists, including, *e.g.,* persons who traveled to Syria to fight for ISIS.

In FY2019 alone, CBP collected biometrics from approximately 79 million arriving foreign nationals. Starting in late 2017, CBP began implementing facial recognition for all foreign nationals (in lieu of finger scans) and, on a voluntary basis, for all U.S. passport holders arriving at U.S. international airports. This innovation has generally been lauded as it expedites immigration processing and limits the interaction with a CBP officer at primary lanes.

As discussed later, establishing Congressionally mandated biometric *exit* has been a far greater challenge for DHS. In 2013, pursuant to legislation, the program office at DHS managing IDENT, US-VISIT, was renamed OBIM, and the responsibility for developing a biometric exit solution was transferred from US-VISIT/OBIM to CBP.[13]

---

[12] Excepting accredited diplomats.

[13] This change occurred pursuant to the *Consolidated and Further Continuing Appropriations Act, 2013* (Public Law No. 113-6). This legislation transferred visa overstay analysis activities, previously performed by US-VISIT, to ICE. The DHS proposed FY 2013 budget went further by contemplating transferring most of the core US-VISIT operations and management of biometric and biographic information storage, matching and watchlist functions to CBP. *See* 2013 Message to Employees: Proposed Transfer of US-VISIT Program.

c. How Biometrics are Currently Being Used by DHS Component Agencies

Biometrics, currently used in various ways by the Departments' operational component agencies,[14] "…is the automated recognition of individuals based on their behavioral and biological characteristics."[iv] The uses for biometrics vary across a wide spectrum to include: identity confirmation, investigative and forensic purposes, background checks, vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification of the identity of foreign nationals seeking to enter the U.S. pursuant to a visa or under the Visa Waiver Program.

As is evident from the above, biometrics, mainly fingerprints (FP), are not new to DHS. However, with US-VISIT and Trusted Traveler programs, such as CBP's Global Entry, their uses have increased over the past two decades, in large part in response to 9/11 and the need to prevent future terrorist attacks on U.S. soil. Moreover, new types of biometrics, such as facial recognition (FR), iris, voice, and DNA, have become more readily available and more reliable in the past decade. Some of these newer biometric modalities, as discussed below, are currently being used by some DHS agencies on a limited basis. As such, it is worthwhile to describe how each DHS component agency utilizes biometrics to accomplish their diverse and often unique missions.

i. U.S. Customs and Border Protection (CBP)

At the front of the pack, as the most prolific and innovative collector and user of biometrics within DHS, is U.S. Customs and Border Protection (CBP), the single, unified border agency for our nation, created as part of the Homeland Security Act of 2002. CBP is primarily made up of two large law enforcement components or divisions. One is the Office of Field Operations (CBP/FO), which manages all of the nation's 328 ports of entry – land, sea and air – for all purposes, including immigration, customs, counterterrorism, counter-narcotics and other contraband. The other is the Border Patrol (CBP/BP) which is responsible for controlling and securing our nation's borders *between* the ports of entry, against illegal migration, drug smuggling, and the like.[15] While the ultimate mission of both is similar, CBP/FO and CBP/BP operate in quite different physical environments. As the nation's largest law enforcement agency, CBP is responsible for securing the borders of our country, at and between U.S. ports of entry, while at the same time facilitating lawful travel and trade through the official entry points.

---

[14] *See* Appendix 3, a grid representing the current uses of biometrics by the operational agencies of the Department.

[15] Primarily in support of CBP/BP, CBP also maintains and operates a fleet of aircraft and vessels under the CBP Office of Air & Marine (CBP/AM). Air & Marine Officers, many of whom are pilots, are also law enforcement officers empowered to make arrests, etc.

CBP Office of Field Operations (CBP/FO)

As noted above, besides collecting and using fingerprints for those it arrests at the border, under the US-VISIT program, CBP's Office of Field Operations (CBP/FO) has used fingerprints to confirm the identities of arriving foreign visitors to the U.S since 2004.

CBP has also made extensive use of biometrics on a voluntary basis in connection with its Trusted Traveler programs, starting with SENTRI and NEXUS at the land borders and, since 2008 with its highly successful[16] Global Entry program.[17] Global Entry has used both finger scans and, since 2018, facial recognition (FR)[18] to identify participants upon arrival at U.S. international airports. Indeed, FR allows for even faster identification of those enrolled in Global Entry and obviates the need for finger scans for those whose prints cannot be easily read due to age or other reasons. Entirely voluntary, Global Entry (similar to its sister CBP programs, NEXUS and SENTRI), costs $20 per year ($100 for a 5-year membership) and involves the collection of fingerprints and a photograph as part of the enrollment process.[19] Once approved, Global Entry members are afforded the benefit of speeding through the federal inspection areas at U.S. airports on arrival via self-service kiosks[20] and at land border POEs via dedicated vehicle and pedestrian lanes. Additionally, Global Entry members are extended the TSA PreCheck™ benefit for the life of their membership at no additional fee.

After being assigned responsibility for biometric exit in 2013, CBP began to consider using facial recognition as a possible solution to implement the longstanding congressional mandate to biometrically identify non-US citizens as they exited the U.S. In 2017, in partnership with the airline industry, which shouldered the financial burden of purchasing, installing, maintaining, and staffing the camera solutions, CBP/FO designed and launched a groundbreaking back-end face matching system called the Traveler Verification Service (TVS). Just before exit (boarding the plane), each international traveler's photo is taken and securely sent to TVS which compares the new photo with those that have

---

[16] Global Entry has proved to be enormously popular. Currently, there are 9.6 million individuals enrolled in Global Entry and its related trusted traveler programs. In FY2019, nearly 13 million travelers, mostly U.S. citizens, were processed via the Global Entry kiosks.

[17] CBP's Global Entry was designed to make immigration and customs processing more efficient for vetted/trusted travelers by providing them a means of self-service immigration and expedited Customs processing. The more individuals who are enrolled, the fewer the number of travelers CBP needs to scrutinize upon entry, *i.e.,* narrowing the haystack.

[18] To address the growing demand for Global Entry and to make the kiosk transaction process even faster and more efficient, CBP began, in 2018, to use facial recognition. Global Entry kiosks were modified so that the photo captured by the kiosk can be used, in lieu of fingerprints and passport scans, to verify the identity of Global Entry members. Facial recognition transactions have reduced kiosk processing time, already short, by an astonishing 90 percent.

[19] To qualify for the expedited process on arrival, GE applicants must provide five years of their travel, employment, and residential address history, and be interviewed in-person by a CBP officer.

[20] Global Entry members are able to utilize a kiosk without the need to stand in a queue to complete their U.S. immigration inspection. They also get expedited treatment through the Customs, or the back end of the Federal Inspection Area, after retrieving their luggage.

been pre-staged in a "gallery" from DHS holdings. The aforementioned "gallery" includes facial images taken during a variety of standard DHS encounters, including those taken by CBP during entry inspections, and photographs from U.S. passports, U.S. visas and other travel documents, as well as photographs from previous DHS encounters. CBP and its airport and airline partners are currently using this facial recognition method for exit in several airports and seaports, with plans to continue expanding to more locations.[21]

However, due to logistical issues relating to separating U.S. citizens from non-U.S. citizens during flight boarding, there is an opt out process available for all travelers, regardless of citizenship. As noted below in Case Study No. 1, privacy advocates still have concerns about taking a photograph of exiting U.S. citizens, even though they can opt out and, in the event a U.S. citizen chooses to participate, their photograph is used for the sole purpose of confirming their identity and is automatically deleted after 12 hours.[22]

CBP Border Patrol (CBP/BP)

The other major operational division of CBP is the Border Patrol (CBP/BP). The CBP/BP mission is similar to CBP/FO, but it operates in a vast and open space of varying terrain at and proximate to the U.S. borders, rather than the closed and structured spaces of the POEs where CBP/FO operates. However, unlike CBP/FO, because it is illegal to cross the border into the U.S. at any place other than a POE, CBP/BP is not responsible for balancing the facilitation of legitimate travelers and the movement of goods into the U.S.

Given its major law enforcement role, CBP/BP collects more biometrics than any other law enforcement organization in the U.S. It annually apprehends nearly half a million aliens who have unlawfully entered the U.S. In carrying out its mission of securing the U.S. borders between the POEs, CBP/BP uses biometrics to identify individuals apprehended in order to determine whether they have been apprehended illegally entering before or are subject to removal or deportation orders [IDENT system] and whether they have a criminal record or are subject to an arrest warrant [NGI system] or are on the terrorist watchlist or are the victim of human trafficking. This collection and use of biometrics, currently only FP, is a traditional use of a well-known biometric post-apprehension.

CBP/BP is not, at this time, using FR for any purpose. However, starting in May 2019, CBP/BP coordinated with ICE/HSI, in what is called Operation Double Helix, to begin taking DNA samples where there was a question of a false claim of parentage by an adult with a minor child. Rapid determinations of parentage (test results take approximately 90 minutes) were and are essential to the safety of the child and to prevent fraud. Indeed, the use of DNA testing for this purpose was one of the emergency recommendations of the Interim Report of the HSAC's Task Force on CBP Families and

---

[21] As described earlier, CBP is also using FR upon arrival at U.S. international airports. Moreover, CBP is testing FR methodology at land border ports of entry (pedestrian and vehicle) for both entry and exit purposes.

[22] U.S. citizen photos captured as part of Biometric Exit are held in TVS for 12 hours for continuity of operations purposes only. They are then deleted.

Child Care issued in April 2019.[23] Since the initiative's inception, 3,356 family units have been tested. As a result of this DNA testing regime, 11% of those claiming parentage were determined to be false.[24]

ii. Immigration and Customs Enforcement (ICE)

ICE consists of two significant divisions. One is ICE Homeland Security Investigations (HSI). The other is ICE Enforcement and Removal Operations (ERO). Both use biometrics.

Homeland Security Investigations

HSI, formerly ICE's Office of Investigations, was created in March 2003 by merging nearly 4,000 U.S. Customs Service special agents with approximately 2,000 INS special agents, and placed within the newly formed agency, ICE. With over 7,000 special agents stationed in over 200 cities across the U.S. and in over 50 countries around the world, ICE's Homeland Security Investigations (HSI) is the largest investigative agency within DHS. HSI investigates, disrupts and dismantles terrorist, transnational and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States. HSI is the investigative arm of CBP and its own sister division, ERO. To accomplish its investigative mission, HSI collects and uses biometrics via a variety of programs, including the traditional, post-arrest booking process described earlier. It also uses biometrics as an investigative tool to assist in solving federal crimes within its jurisdiction.

One such program is the Biometric Identification Transnational Migration Alert Program (BITMAP).[25] BITMAP is an investigative tool that utilizes biometric information captured and shared by foreign law enforcement partners to identify terrorists and transnational criminals and disrupt their illegal activity. Another, the previously discussed Operation Double Helix, is the initiative with CBP/BP taking place on the southwest border of the U.S. with the aim of detecting, investigating and prosecuting adults fraudulently claiming parental relationships with unrelated minors to secure their own entry into the U.S. The focus of HSI's Operational Technology and Cyber Division (OTCD) is on

---

[23] *See* HSAC Families and Child Care Interim Report, page 9, Recommendation No. 2a. As tender aged children from Central America were being exploited and "re-cycled" with multiple entities by different persons posing as a parent, the HSAC Panel recommended that an existing DHS regulation, 8 CFR Section 235.1, be changed to allow CBP to take photographs and biometrics of children under 14. This recommendation, which is necessary to determine whether a child is being re-cycled, would also provide evidence against smugglers exploiting tender aged children for this purpose. The proposed regulatory change has yet to be implemented.

[24] Of those family units tested, 287 produced negative results (8.5%) for a parent/child familial relationship. Additionally, 121 of the persons who claimed parentage confessed to being fraudulent prior to testing. To date, 390 individuals have been referred to DOJ for prosecution with 234 being accepted for prosecution. Of note, once the test is complete, regardless of the outcome, the physical DNA is destroyed. No DNA information obtained through Operation Double Helix is currently uploaded into the Combined DNA Index System (CODIS) or any other database.

[25] BITMAP is explained in greater depth below, in section VI of this report.

merging methods and technology that result in better law enforcement operations. As part of that, OTCD's Law Enforcement Information Sharing Initiative (LEISI) works to coordinate information sharing, including biometric information, among domestic and international law enforcement partners. Additionally, OTCD's Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement (EAGLE) is the primary database within ICE for booking, searching, and entering a subject's biometric information. Finally, the HSI Victim Identification Program (VIP) within the Child Exploitation Investigations Unit (CEIU), which investigates the trafficking in child pornography and exploitation of minors, utilizes fingerprints and facial recognition with both photographic images and videos from ongoing criminal investigations to identify offenders and their child victims.

Enforcement and Removal Operations

ICE's Enforcement and Removal Operations (ERO) arrests and manages aliens already in custody, often after arrest by CBP/BP, and removes individuals from the U.S. who have been ordered removed, either via expedited removal proceedings or order of deportation. Thus, ERO agents take biometrics, primarily fingerprints, to identify those who are transferred to its custody. Its biometrics are submitted to OBIM's IDENT.

As for programs using biometrics, like HSI, ERO also shares the use of the EAGLE platform as a biometric database. As part of that, ERO uses the EAGLE DirecteD Identification Environment (EDDIE), a mobile application, to either collect 2 fingerprints manually or 10 fingerprints via a photo, to identify subjects through IDENT. ERO also uses its Alien Criminal Response Information Management tool (ACRIMe) to assist them in better tracking cases in which they have a stake. ACRIMe is a web-based system designed to increase efficiency in the identification and prioritization of persons of interest to ICE. ACRIMe enables biometric interoperability between OBIM's IDENT and the FBI's NGI database. As such, ACRIMe allows ERO to receive notifications related to persons of interest and respond to immigration status inquiries made by other agencies about individuals that have been arrested, are subject to background checks, or are otherwise encountered by those agencies. ERO also collects DNA to help more effectively track subjects undergoing criminal prosecution via their Prosecutions Module. In addition, ERO has deployed the Compliance Assistance Reporting Terminal (CART) to several field office locations. CART is a self-service machine that conveniently captures a photo and four fingerprints to check for wants and warrants of those under ICE orders of supervision, thus reducing the number of individuals needing in-person attention at an ICE office. Finally, on a limited pilot basis, ERO has recently begun collecting DNA on all aliens taken into custody for immigration violations, not just those held for criminal prosecutions. This pilot is currently only deployed to the ERO office in Dallas, Texas.

iii. U.S. Citizenship and Immigration Services (USCIS)

United States Citizenship and Immigration Services (USCIS) administers the nation's lawful immigration system and investigates and adjudicates applications for change of status, permanent resident alien status and U.S. citizenship, but is not a law enforcement agency. To do this, USCIS adjudicates requests for immigration benefits, processes applications to sponsor relatives and future spouses, as well as refugees. In addition, USCIS is the agency that processes applications for U.S. citizenship, grants Lawful Permanent Resident (LPR) status and issues the associated "green cards". It also organizes and hosts new U.S. citizen naturalization ceremonies. As part of its functions, on an average day in 2019, USCIS collected fingerprints and photographs of approximately 14,000 people at their 133 application support centers. USCIS uses IDENT and NGI in order to do background checks on alien applicants for LPR status and U.S. citizenship. As noted earlier, USCIS has recently issued a Notice of Proposed Rulemaking that, if adopted as a final rule, would expand its authority to collect and use other biometric modalities to identify applicants on a person-centric basis, and in some situations authorize the collection of the biometrics of U.S. citizen sponsors of applicants seeking immigration benefits.

iv. Transportation Security Administration (TSA)

The Transportation Security Administration (TSA), a relative newcomer to the practice of collecting biometrics for operational purposes, generally has not and does not use biometrics as part of its airport passenger screening function. But TSA also has a credentialing mission involving those who work in, or have access to, secure areas of airports, or who transport hazardous materials. Additionally, background checks are conducted as part of TSA's Alien Flight Student Program (AFSP) which helps ensure that non-U.S. citizens taking flight training in the U.S. do not pose a threat to aviation or national security. Biometrics, exclusively fingerprints, are used to conduct the background checks relevant to TSA credentialing programs.

Regarding its passenger screening mission, early in FY 2020 TSA began deploying Credential Authentication Technology (CAT) units in airports across the U.S. to address ID fraud vulnerabilities. CAT verifies the security features on a traveler's ID and provides automated access to real-time Secure Flight traveler vetting information at the checkpoint. CAT improves the detection of fraudulent documents and allows TSA to screen passengers more effectively on a risk basis.

Beyond that, TSA is taking a phased approach to test 1:1 (one to one) facial recognition capabilities by integrating a camera with existing CAT machines (CAT-C) to verify a live image capture against the image on a credential, usually a driver's license. In September 2019, at McCarran International Airport (LAS) in Las Vegas, TSA conducted a 30-day pilot using CAT-C with volunteer TSA PreCheck™ passengers. After LAS, TSA spent nearly a year refining the technology with the vendor and industry experts.

In light of COVID-19, advanced health and safety precautions, including contactless identity screening, have become a priority and part of the new normal for TSA and the travel industry. As a result, TSA is exploring rapid testing and deployment of self-service technologies at airport

checkpoints, particularly at the Travel Document Checker (TDC) entry point. In August 2020, TSA started piloting the self-service version of CAT-C (CAT-2) at Ronald Reagan Washington National Airport (DCA) with volunteer passengers. CAT-2 will allow passengers to scan their own identity document for authentication and will automatically capture a photo for facial recognition, vastly reducing unnecessary contact between Transportation Security Officers (TSOs) and passengers. This technology will help improve the accuracy of the identity verification process, lower TSA's reliance on the boarding pass, and enable a near-real time connection to TSA vetting systems for up-to-date results. It should be noted that each photo taken as part of CAT-C and/or CAT-2 is overwritten and thereby deleted when the photo of the next traveler is taken or when the TSA officer logs off the machine.

TSA, working in conjunction with CBP, is operating a limited pilot at Hartsfield Jackson International Airport in Atlanta whereby internationally bound travelers have their photo taken at the TDC, which is the ID checking phase of the TSA process. That photo is sent to CBP's TVS for matching, and if a match is found, that traveler is not required to present any form of ID, which makes this process faster than either the CAT-C or CAT-2. If there is no match, the traveler will have their ID verified manually by the TSO staffing that TDC podium. Those captured photos, as with the CAT-C and CAT-2 facial recognition tests, are not retained by either TSA or CBP.

TSA also operates their voluntary, and highly successful, PreCheck™ program which, like Global Entry, involves the collection of fingerprints and a photograph as part of the enrollment process. There are presently more than 380 PreCheck™ enrollment centers nationwide that are operated by private companies via contracts with TSA. When applicants provide their background information and biometrics as part of the enrollment process TSA securely transfers that data into IDENT for storage. PreCheck™ enrollment data (biographic and biometric) for the vast majority of applicants is stored for the life of that traveler's membership plus one year. In the event that derogatory criminal and/or terrorism related information is uncovered during the background check, the data is subject to longer term retention. PreCheck™ status, which can also be acquired by enrolling in CBP's Global Entry, costs $85 for a 5-year membership and provides the benefit of quicker moving queues and less invasive pre-board security screening.[26]

[26] Operating within the TSA screening space at more than 30 major airports in the U.S., CLEAR is a privately owned and operated program that offers members front of the line privileges at TSA screening queues for $179 per year. To enroll, travelers must provide biographic and biometric information, the storage of which is managed solely by CLEAR. CLEAR maintains all member data (biometric and biographic) until the membership is terminated *and* the member submits a request with CLEAR to have their information deleted. CLEAR does not conduct any background checks on their members as their program is a Registered Traveler Program (as opposed to a Trusted Traveler Program) which is designed only to validate their members' identity, not to assess their risk.

v. United States Secret Service (USSS)

An agency with 3,200 special agents and 1,300 uniformed security personnel, United States Secret Service (USSS) has two missions. The best known, and the one that gave birth to the USSS, is the protection of the President and visiting heads of state. But USSS also is a federal investigative agency with jurisdiction to investigate the manufacture of counterfeit currency, credit card fraud, and related federal crimes.

As a law enforcement and investigative agency, USSS uses biometrics in ways similarly to HSI, mostly employing them in arrests and booking procedures as well as in support of criminal investigations. More than just fingerprint collection though, USSS also collects facial images, palm prints, and situationally, DNA.

vi. U.S. Coast Guard (USCG)

As most of its law enforcement activities occur at sea, the United States Coast Guard (USCG) operates in a unique environment as compared to its DHS counterparts. Still, the USCG has apprehended 374 suspected drug smugglers through the 3rd quarter of FY 2020 and has seized 331,090 lbs. of illegal drugs being carried on vessels of all types and sizes. The USCG determines the identity of those arrested on vessels carrying contraband or engaged in other illegal activity by collecting fingerprints and facial images via mobile devices. These biometrics, mainly fingerprints, are run against IDENT and NGI in order to conduct background checks on those interdicted and/or arrested at sea.

d. Several Departmental Support Offices Play Significant Roles Regarding Biometrics

Besides the DHS operational agencies discussed above, several departmental-level offices play a role in biometrics, including biometrics policy and/or coordination. They include:

i. DHS Management Directorate

The Management Directorate has several offices that play a role in coordination and implementation of biometrics with DHS. The two principal offices are the Office of Biometric Identity Management (OBIM) and the Budget Office. Also, tucked within the Management Directorate is the Federal Protective Service (FPS).[27]

[27] The Federal Protective Service (FPS) is charged with protecting federal property, principally federal buildings. Because of its small size and budget, unlike the other DHS operational agencies discussed above, FPS has never been a standalone operational component of DHS. Rather, FPS was a part of ICE until 2009. In 2009, FPS was moved to the National Protection and Programs Directorate which was then transformed into the Cybersecurity Infrastructure Security Agency (CISA) in 2018. As a result of the creation of CISA, since 2019 FPS has been aligned under the DHS Management Directorate. FPS largely relies on the 13,000 contract security personnel hired primarily as security screeners to protect the 9,000 federal facilities for which they are responsible. FPS has only 1,300 direct hire employees. In terms of use of biometrics in support of its mission, FPS collects fingerprints from arrestees and job applicants. It does not, at this time, use facial recognition.

Office of Biometric Identity Management

Aligned under the Management Directorate at the DHS headquarters level, Office of Biometric Identity Management (OBIM) is the backbone for much of the Departments' biometrics related operations. As noted earlier, OBIM is the successor to the US-VISIT office which assisted CBP in its efforts to gather biometrics on foreign nationals seeking to enter the U.S. Since 2013 OBIM has been aligned under the DHS Management Directorate.[28]

Currently, OBIM's primary responsibilities are to provide biometric storing, sharing, and analytical (biometric matching) services to all DHS agencies and to other agencies of our government. To accomplish this, OBIM manages IDENT, DHS' biometric repository and multi-modal matching system, as well as the Biometric Service Center (BSC), which provides biometric identification and verification 24 hours a day, 7 days a week. Currently, OBIM is developing IDENT's replacement system, Homeland Advanced Recognition Technology (HART), which will, among other things,[v] expand its ability to store and manage biometric modalities, beyond FP, FR and iris, to include DNA and voice recognition. Lastly, pursuant to the Department's international sharing agreements, OBIM helps identify victims of terrorist attacks and natural disasters around the globe.

Budget Office

The Management Directorate (MGMT) not only houses OBIM, as described above, but importantly it oversees the Department's budgeting process. For budget formulation and execution, biometrics are typically associated with specific programs rather than as standalone line items in DHS agency budgets. Still, as discussed below, the DHS budgeting process is an important coordinating mechanism within the Department for, among other things, the acquisition, use and storage of biometrics.

ii. DHS Office of Policy

When DHS was created in early 2003, there was no office of policy and planning at the Department headquarters level. In 2005, this omission was rectified and the Office of Policy (PLCY) was created under a DHS Assistant Secretary. PLCY plays a key role within the Department in translating the DHS Secretary's vision into policy. It also develops department-wide policy, applicable to all component agencies, as needed. It identifies where there is mission overlap between component agencies and, after a vetting process, recommends to the Secretary any clarifications of roles and responsibilities that are needed. Needless to say, all these roles apply to the use of biometrics by DHS operational agencies, including the use of new types of biometrics or novel uses of existing biometrics to support missions of the Department or individual component agencies. In addition, PLCY has played a lead role within the Department in negotiating international biometric data sharing arrangements.

[28] The Subcommittee considered whether OBIM was optimally placed within the DHS organizational structure. See discussion in section VIII, below.

iii. DHS Science and Technology Directorate (S&T)

The Science and Technology Directorate (S&T) was created by Congress in 2003 as one of the five "directorates" of DHS. S&T promotes and sponsors Research, Development, Test, and Evaluation (RDT&E) and works in partnership with the National Institute of Standards and Technology (NIST) and other research institutions to, as it pertains to biometrics, evaluate facial recognition, iris, touchless fingerprint capture technologies, and other emerging identity and biometric technologies. In a broader sense, S&T works to support the DHS operational agencies' potential needs for cutting edge technologies in support of their missions.

iv. DHS Privacy Office

The Privacy Office (PRIV) was established in 2003 as the first statutorily created privacy office for a department of the federal government. PRIV's primary mission is to protect the privacy of all individuals consistent with laws and regulations and to enable the Department to better manage threats while simultaneously protecting personal privacy and promoting accountability, transparency, and public understanding of the Department's activities through strategic advice, oversight, and disclosure. Any time any DHS initiative, system, or program uses or proposes to use personally identifiable information (PII), including new uses of biometrics or novel uses of existing biometrics, PRIV's role is to be part of the process to ensure that privacy concerns are addressed. PRIV reviews new or proposed technologies used, or proposed to be used, by the Department's operational agencies to ensure they uphold, rather than potentially erode, privacy protections. To carry out its functions, PRIV liaises with the Privacy and Civil Liberties Oversight Board (PCLOB), the Federal Privacy Council, and the Data Privacy and Integrity Advisory Committee (DPIAC), among others, on privacy matters, issues, and trends. Finally, PRIV responds to complaints of privacy violations submitted to the Department and facilitates redress, as appropriate.

v. DHS Office of Civil Rights and Civil Liberties

The Office of Civil Rights and Civil Liberties (CRCL) was established by the Homeland Security Act of 2002 with an overall mission to serve the DHS, by preserving individual liberty, fairness, and equality under the law. With respect to biometrics, CRCL advises DHS leadership on policy creation and implementation to ensure civil rights and civil liberties are actively promoted. CRCL also works closely with OBIM to ensure technical methods do not undermine confidentiality provisions, and to develop biometrically focused person-centric identity strategies that remain supportive of standards for record matching, proper handling of sensitive data, and access controls. In addition, CRCL participates in several DHS enterprise-level groups working on biometric issues, including the Biometric Capabilities Executive Steering Committee (BC-ESC).

III. DHS' Current Oversight and Coordination Mechanisms

a. Organizational Structure of DHS

When it comes to using biometrics in aid of a mission, each individual DHS operational component evaluates whether a biometric would be useful and how such biometric capability not only furthers or enhances one of its missions, but how it can be integrated into the agency's operations. A key issue is what operational protocols will be needed to accompany the introduction of the biometric. The latter is often called the "concept of operations" or "CONOPS." Thus, the primary responsibility for developing and vetting a new use of a biometric is vested in the DHS operational agency. We see no reason to change this. Indeed, removing the vetting and decision making from the operational component would likely create serious dysfunctions.

Yet the Subcommittee's taskings pose the question of what the Department's role should be in coordinating and providing oversight of one or more component agencies' use of a new biometric or a novel use of an existing biometric. To understand the Department's optimal role requires an appreciation of how DHS, now nearly 18 years in existence, has historically performed this function, not just with respect to biometrics, but as to other potentially important operational improvements that facilitate agency missions. From a public administration or governance point of view, this requires an understanding of the organizational structure of DHS, as a department of our federal government.

Structurally, unlike the oft repeated statement in the media dating back to the origins of the Department, DHS is not an actual merger of 22 agencies. It is not now, and it never was. The only actual mergers of people and functions triggered by the Homeland Security Act of 2002 were limited to CBP[29] and ICE.[30] The original seven operational agencies created as a result of the homeland security reorganization of 2003 were aligned under the new Department, but they were not merged. They are CBP, USCG, TSA, ICE, USSS, USCIS and FEMA. *See* Figure 1: DHS Organizational Chart, p. 7, above. The DHS component agencies,[31] which now includes CISA, share a broad goal to help protect the U.S. homeland; but even their homeland security missions differ significantly and most have traditional missions that are unique and unrelated to counterterrorism.

From the beginning, DHS, at the department level, established oversight of the Department's operational agencies through an organizational structure whereby the head of each of the seven operational agencies reported to the Secretary of DHS (S-1), usually through the Deputy Secretary (S-2), who functions in the nature of a chief operating officer and has day-to-day oversight of the

---

[29] CBP is a merger of most of U.S. Customs with frontline elements of the former INS - - both immigration inspectors at the POEs and the entire Border Patrol as well as agriculture (APHIS) inspectors from the Department of Agriculture who were stationed at ports of entry.

[30] ICE is the merger of elements from the former INS charged with interior immigration enforcement, detention and removal and Customs special agent investigators.

[31] 98%-99% of the DHS' 240,000 personnel are employed by these eight component agencies. Approximately three-fourths of DHS' total personnel are employees of three component agencies: CBP, TSA, and USCG.

Department's support offices and its component agencies. Thus, department oversight and coordination are accomplished through an operational chain of command that extends from the Secretary down to and through the agency heads. Superimposing structures that break this chain of command have typically resulted in dysfunction or have been ignored.[32]

Thus, in accordance with the Department's organizational structure, to secure policy and budgetary support for a new program, whether or not it involves biometrics, has typically required the presentation of an implementation plan or proposal to S-2. Especially in the early years of DHS, such presentations were vetted through S-2's informal, but regular "Gang of 7" meetings.[33] This process enables other agency heads to have visibility and to raise any issue of overlap, and if there is overlap, for DHS leadership, as part of its coordination role, to designate which of the DHS component agencies would be given the lead.[34] Besides ensuring that new programs are briefed and receive the endorsement of top DHS leadership, without such a vetting process, an agency head could not be assured of the needed budgetary support for any significant new undertaking. This process generally has served the Department well. It has provided both coordination and oversight without cutting line authority from S-1/S-2 to the agency head, who ultimately must be held accountable and responsible to the Secretary.

b. The DHS Budget Process

In addition to the DHS organizational structure, another vehicle for coordination and oversight by the Department for all programs, including those involving biometrics, is the budget process, discussed above. The budget function at the departmental level is within the Management Directorate (MGMT). The DHS budgeting process is an important coordinating mechanism within the Department for many programs and functions, including the acquisition, use, matching, storage and protection of biometrics.

Within MGMT, the Program Analysis and Evaluation Division (PA&E) runs the Department's program and budget review process. Working with PLCY, PA&E issues top line budget guidance to each component agency months before the Department's budget request is submitted to OMB. Each DHS component agency and departmental-level support and programmatic office submits its proposed budget request, broken down by programs, to PA&E and MGMT's Budget Division. It is then subject to a presentation by the agency head and a vetting process over the next several months in advance of the DHS proposed budget submission to OMB. Ultimately, there is a review and pass back process from OMB that results in the President's budget for the entirety of the Department.

---

[32] As can be seen, the DHS structure is more similar to DOJ structure than the DOD. Yet occasionally a DHS Secretary has looked to the DOD model of joint commands, even though they undermine the chain of command and are inconsistent with the DHS organizational structure.

[33] This informal process was later formalized with the creation of the Deputy's Management Action Group (DMAG).

[34] E.g., this process was used regarding Global Entry. CBP proposed Global Entry to S-2 in 2005. Its implementation was temporarily delayed by S-2 in order to determine whether CBP's enrollment software for vetted Global Entry participants could be leveraged and used by TSA which was in the process of developing its own trusted traveler program, ultimately called PreCheck™. Thus, the Department played an appropriate and important coordination and oversight role.

This process identifies significant overlaps where they exist. While not specifically geared toward coordination and oversight of biometrics, the Department's budget review process is an important existing mechanism for eliminating overlap and ensuring coordination of all programs of DHS operational agencies, including those using biometrics.

One of our recommendations is that, as part of each agency budget proposal, budget guidance direct component agencies to indicate which of its programs use biometrics. This will increase department-level visibility of the use of biometrics and potentially flag issues of overlap. *See* Recommendation No. 10.

c. DHS Acquisition Review Board

The DHS Acquisition Review Board (ARB), formally created in 2019,[35] is chaired by the Under Secretary of Management and consists of individuals who manage the Department's missions, objectives, resources, and contracts, among other things. The ARB meets regularly to review major acquisition programs to enhance accountability and uniformity in the review process as well as to ensure proper management and oversight of said programs. As it pertains more specifically to biometrics, the ARB serves to ensure that when major procurement efforts are made for biometric technologies from one DHS operational agency or component, the other components are informed so they may, if needed, join in on the purchase to reduce overlap and improve DHS' purchasing power.[36]

d. DHS Biometrics Strategic Framework (2015-2025)

DHS has implemented several mechanisms that are directly related to biometrics coordination. One such effort led to the DHS Biometrics Strategic Framework, 2015-2025, dated June 9, 2015 (DHS Biometrics Framework). This document, produced by a DHS intra-agency process, was intended "to establish the overarching vision for how enhanced biometrics capabilities will transform DHS mission operations over the next ten years." It is an ambitious document, but clearly aimed at establishing an overarching vision for DHS and its component agencies. It envisions the "re-architecture of IDENT" (something that is coming to pass as OBIM evolves IDENT into HART) and recognizes "various biometric initiatives being implemented by DHS Operational Components." Framework, p. 3. The Framework provides a useful statement of DHS' mission and goals, and includes sound objectives, such as, refining "processes and policies to promote innovation using biometrics." This Framework makes a number of recommendations for how to assess and coordinate overlapping multi-agency biometric requirements, integrate privacy policy and law into new biometric collections and uses, and

[35] On June 12, 2019, the U.S. Congress amended the Homeland Security Act of 2002 via House Resolution 2609, to formalize the DHS Acquisition Review Board (ARB).

[36] To underscore the importance and value of the ARB, a recent Government Accountability Office (GAO) report found that the "Department of Homeland Security (DHS) plans to invest more than $7 billion in major acquisition programs each year from fiscal years 2020 through 2024…".

enhance stakeholder communications[37] to ensure a more complete understanding of DHS requirements in the biometric space. The Framework also includes recommendations to implement standardized solutions, eliminate duplicative support services, and establish appropriate oversight in order to ensure that the offices of PRIV and CRCL are looped into the oversight structure. Framework, pp. 10-11. Although its overall vision and goals are well articulated, including, e.g., person centric biometric operations for USCIS and enhancing IDENT, most of the Framework's recommendations have yet to be implemented.

One of our recommendations is to update the 2015 Biometrics Strategic Framework in light of this report. *See* Recommendation No. 6.

e. DHS' Biometric Capabilities – Executive Steering Committee

The Biometric Capabilities – Executive Steering Committee (BC-ESC), started in 2018, is currently the only continuous DHS-wide body focused on biometrics. Chaired by the Deputy Under Secretary for Management, it is supported by a secretariat within OBIM. The mission of the BC-ESC, according to its charter, is "to provide governance, oversight, coordination, and guidance to all DHS and Component-level programs that are developing or providing biometric capabilities" in support of mission objectives. Meeting quarterly, the BC-ESC includes broad participation across DHS, to include SES-level representatives from all relevant DHS operational agencies and on the department-level from OBIM, CRCL, PRIV, OGC, Office of the Chief Information Officer, Office of the CFO, Office of the Chief Procurement Officer, Office of Policy's Office of Strategy, Policy and Plans, and the Joint Requirements Council. It has recently been the forum at which the DHS intra-agency received briefings on facial recognition issues and biometric updates, such as its uses, pilot projects, and contactless biometrics programs. Action items coming out of this DHS executive steering committee include greater collaboration on facial image quality standards, privacy issues, and an array of research and development initiatives.

In the Subcommittee's view, this intra-agency biometrics steering committee, comprised of representatives from all DHS components with equities in biometrics, serves a valuable function that should continue. That said, the BC-ESC is not well suited to develop high-level department-wide policy, when such policies are needed, for new programmatic uses of biometrics. Nor can the BC-ESC direct that coordination to take place between DHS operational agencies when that is appropriate. In addition, it is not currently charged with reviewing and vetting implementation and communication plans where one of the DHS component agencies is proposing to use a new biometric or an existing biometric in a new way in furtherance of one of its missions.

For these reasons, the Subcommittee concludes that there is a need for a DHS Biometrics Oversight and Coordination Council (BOCC), chaired at a higher level, *i.e.,* by the DHS Deputy Secretary, who

---

[37] The communications discussed in this 2015 Framework relate to improved communications to set forth DHS requirements, not explanatory outreach before implementation of the new or novel uses of biometrics. This evidently was not an issue 5 years ago.

has line authority over the heads of the DHS operational agencies. *See* Recommendation No. 1. However, we believe that the BC-ESC could still play a valuable intermediary role and that, if properly utilized, it would complement the BOCC without being duplicative. As we envision it, the BC-ESC would remain an intra-departmental biometrics working group that would not only give department-wide visibility into individual agencies' programmatic uses of biometrics, but would serve to triage issues involving biometrics, rapidly identifying those that need to be taken to the BOCC for resolution. Moreover, the BOCC could task the BC-ESC to study and develop recommendations relating to proposed uses of biometrics.

f. December 2019 Delegation to Under Secretary for Strategy, Policy, and Plans

In December 2019, the Acting Secretary of Homeland Security issued a delegation of authority to the head of DHS' Office of Policy, dated December 9, 2019. While this 9-page delegation of authority is by no means limited to the uses of biometrics by DHS operational agencies, it delegates, subject to the Secretary's direction and guidance, the Secretary's authority to Policy "to lead, conduct and coordinate the development and implementation of department-wide strategies, policies, and strategic planning to promote and ensure quality, consistency, and integration for the programs, Components, offices and activities across the Department." "Biometrics is explicitly included among the 12 topic areas listed in the delegation. *See* Delegation, II.A.5.

During the course of the Subcommittee's extensive interview process, few individuals outside of PLCY were aware of this delegation. Under the delegation, PLCY represents DHS at "interagency committee meetings relating to the broad set of issues, Delegation II.C, including, *e.g.*, immigration and border security (II.A.2), and transportation and cargo security (II.A.5). Ideally, PLCY will include the DHS operational component that has the lead on these missions in interagency policy meetings on these subjects. It also appears that PLCY is clearly designated as the lead negotiator for agreements between and among other federal, state, local, tribal, foreign governments, and international organizations, including agreements related to the sharing of biometric information. Delegation, II.E; II.J.4 and II.J.5; II.M.5. As PLCY has historically been the lead DHS negotiator for biometric data sharing arrangements, this part of the delegation appears to be merely a re-affirmation of this role; however, the other delegations related to biometrics do not appear to have been implemented at the time of this report.

The Subcommittee notes that the Acting Secretary's December 2019 delegation vests in the Under Secretary for Policy, the role of "leading and developing Department strategies, policies and plans regarding the collection and use of biometrics." II.M.4. Representatives from PLCY advised that several options are being considered for implementing this delegation. The options being considered include the use of a Program Management Office (PMO) within the Policy Office to manage and direct DHS component agencies' uses of biometrics to support various agency missions. For the PMO, all new uses of biometrics would have to be approved by the PLCY program manager/coordinator. Also, under consideration is what is unofficially described as "PMO Lite," which we understand would be the proposed PMO with the exception that PLCY would not operate and maintain the IT systems relating to biometric collection. Another option would be an intra-agency coordination model for

vetting biometrics, including new uses of biometrics within operational agency programs.

As this delegation is quite broad, we are reluctant to comment on any aspect of it that goes beyond the collection, uses, purposes, storage, protection, and sharing of biometrics. The Subcommittee believes that the Department's existing governance/organizational structure, its budget process, the BC-ESC together with a high-level BOCC, as recommended by the Subcommittee, are sufficient to manage, coordinate and provide oversight of the use of biometrics by DHS and its operational agencies. We would be concerned if the development and use of biometrics were driven by a department-level support office rather than individual operational agencies. Not only would a PLCY directed regime likely stifle innovation, it is not consistent with the organizational chain of command of the Department. In our experience, delegation of line authority below the S-2 level diminishes the ability to hold heads of component agencies accountable.

IV. What is the Problem We Are Trying to Fix?

A wise, former DHS official used to start meetings, before allowing the Power Point presentation to begin, with a simple question: "Tell me, what is the problem we are trying to fix?"

Throughout the course of the Subcommittee's extensive interview process, we have asked that question, in one form or another. We gleaned that there is some controversy surrounding some of the new uses of biometrics and identified some friction between DHS operational agencies and between agencies and departmental offices relating to biometrics.

Biometrics have a long and successful history within the DHS. Starting with the building of a biometric entry capability in 2004 and winding its way through the inclusion of facial recognition into Global Entry kiosks in 2018, biometrics have been a catalyst for change in DHS that have ultimately made a variety of DHS missions more successful and processes more efficient, effective, and secure.[vi] But there have been some bumps in the road along the way. At least one new use of biometrics, FR, has stirred controversy within and outside of the Department.[vii] In addition, the lack of clearly defined roles has caused some friction between DHS headquarters-level offices and DHS operational agencies. For example, it appears to the Subcommittee that one of the issues that drove our taskings relates to the strong reaction from privacy advocates and the Hill regarding CBP's use of FR as part of its Biometric Exit program. In addition, as the vast majority of DHS' overseas offices are headed by ICE/HSI Attachés, which obtain and share law enforcement information with its foreign law enforcement counterparts, some tension has developed over the Department's negotiation and terms for sharing biometric information led by PLCY. Concerned about any infringement on its area of expertise, OBIM objected to CBP performing FR biometric exit matching within CBP's TVS system. Moreover, while relationships between CBP and TSA have been generally good, there is a belief that greater coordination between these two important operational agencies of DHS could yield benefits, which may require more direction from above.

The "problems" referenced above are best illustrated by three "biometrics" case studies, described below. These case studies illuminate our recommended solutions. Because facial recognition has ignited much of the concern, some background regarding FR is necessary.

Background regarding Facial Recognition

Despite the highly successful and non-controversial (as it involves consent) introduction of FR as part of CBP's Global Entry program, one of the issues that emerged from the Subcommittee's interviews was the use of relatively new biometrics like facial recognition (FR) as a biometric identifier. The collection of biometrics, regardless of modality, is potentially a privacy-sensitive issue, especially for U.S. citizens where privacy laws come into play.[viii] Some privacy advocates have suggested that law enforcement agencies be prohibited from using FR altogether. In particular, some have advocated that DHS suspend all use of FR for any purpose, pending further study.[38]

Facial recognition does, indeed, pose a unique set of privacy concerns. For instance, it is possible for photos to be taken at a distance, covertly, and without consent of protesters exercising their First Amendment rights. Also, as the technology underscoring the practice of FR is relatively new, and because the National Institute for Standards and Technology's (NIST) ongoing Facial Recognition Vendor Test (FRVT) has demonstrated differences in reliability for certain demographics depending on the matching algorithm, it is crucially important that privacy standards be appropriately maintained and that the choice in matching algorithm be made to ensure the highest rate of accuracy available across all demographics when FR is used. Because a recent report on the FRVT contributed to concerns over the use of FR, the Subcommittee interviewed the lead author of that report[ix], NIST Computer Scientist, Patrick Grother, to gain a better understanding of this issue. Before further discussion of DHS' uses of FR, it is important to digress for a moment to discuss NIST and its work, especially NIST's December 2019 FRVT report.

National Institute of Standards and Technology (NIST)

Currently situated in the Department of Commerce, NIST's[39] work includes measuring and assessing many different biometric modalities and the standards surrounding them. In its December 2019 report, NIST detailed the results of some of its ongoing research into FR via their "Face Recognition Vendor Test Part 3: Demographic Effects" (FRVT). The reports lead author, Patrick Grother, briefed the subcommittee on NIST's testing methods and results and discussed the subsequent interpretation by outside organizations, specifically because the results raised concerns in the media and with privacy Non-Governmental Organizations (NGOs) regarding whether FR technology is inherently biased.[x] More specifically, NIST's FRVT evaluated the performance specific to demographic differences among 189 matching algorithms. The report concluded that, while the majority of the algorithms demonstrated large variations in demographic matching performance, the leading contemporary

[38] e.g., the "Facial Recognition and Biometric Technology Moratorium Act of 2020" introduced by Senator Edward Markey on June 25, 2020 and the January 27, 2020 letter to PCLOB and Congress from 40 consumer, privacy, and civil liberties organizations.

[39] NIST currently has over 3,000 federal employees. It was founded by congress in 1901 to establish a measurement and standards laboratory. NIST's work includes material measurement, physical measurement, engineering, information technology, communication technology, nanoscale science and technology, neutron research, computer security, and, importantly to this Subcommittee, biometrics.

algorithms (like those used by CBP) were highly accurate and did not exhibit statistically significant demographic matching variances.

Although the misinterpretation of those results by the media and privacy NGOs is understandable, it is important to set the record straight. To put it plainly, yes, the majority of face matching algorithms do exhibit bias and less than acceptable matching results; however, this is not true for *all* face matching algorithms.[xi] Many of those that performed poorly are likely still in various, if not early, stages of the development process. However, the matching algorithm used by CBP (which was, and is still, part of NIST's testing), does *not* exhibit bias and was shown to be one of the most accurate of all algorithms tested[xii]; more accurate than humans, such as CBP officers, determining, at a port of entry, whether a traveler is a match to the document presented (e.g., passport, visa) or not.

It is worth noting that face matching algorithms themselves cannot technically be biased. They do not notice color of skin, gender, or age. Every matching algorithm is merely a product of the facial images on which it was trained[xiii], which is simply a representation of whatever images the developer was able to procure.[40] Therefore, one of the promising benefits of the use of biometrics, if properly developed and deployed, is the *reduction* in potential racial bias that can occur either consciously or unconsciously from human subjectivity.[xiv]

During Mr. Grothers' Subcommittee briefing, he noted that the growth of face matching algorithms has undergone a massive expansion in recent years, that accuracy varies across countries and industries, and that the highest performing algorithms continue to improve and are also increasingly tolerant of low-quality images; meaning that the field of FR has grown, and continues to grow, and improve in great strides. In summary, while all face matching algorithms are not created equal, it is the responsibility of the end-user to ensure a frequently tested, highly accurate algorithm is chosen. The Subcommittee found no evidence that a poorly performing algorithm is being used anywhere in DHS, but rather the contrary.

With this background in mind, it appears that one of the issues that drove the Subcommittee's taskings relates to the concerns of privacy advocates regarding CBP's use of FR as part of its Biometric Exit program. For that reason, we discuss this program as the first of our three case studies.

---

[40] Generally speaking, algorithms developed in, for example, Asia, are likely to have been "trained", largely, on facial images of Asian people as those photos would have been more readily available. This, depending on how nuanced the algorithm, could cause the resulting performance of that face matching algorithm developed in Asia to be perceived as "biased" due to its inability to match non-Asian faces as well as it can match Asian faces. Again, as noted, this is *not* true for all algorithms, but rather is used as an example to provide a better understanding of how algorithms are developed and why some of them exhibit such differing degrees of demographic performance.

a. Case Study No. 1: CBP's Use of Facial Recognition for Biometric Exit

Partly because of the aforementioned December 2019 NIST FRVT report and partly because of privacy concerns inherent in FR, there has been much discussion among privacy groups and in the media regarding CBP's use of FR to implement the long-standing Congressional Biometric Exit mandate.[xv] Indeed, CBP officials have testified on this subject before Congress at least six times in the past three years. Accordingly, it is worthwhile to explain what prompted CBP to initiate biometric exit using FR, what steps it has taken to ensure the privacy of all travelers is protected, and under what authorities it is operating.

At the outset, it should be noted that CBP's Biometric Exit operation is not the implementation of a new process but is merely the automation of an existing one. All internationally bound passengers exiting the U.S. have long been subject to identity checks and potentially to checks for outbound currency (in excess of $10,000) and contraband prior to boarding. This is part of CBP's broad border authority. CBP's use of FR for exit is limited. It is only being used to verify identity, *i.e.*, that the person exiting is the person who was issued a visa to enter in the first instance or is the person depicted on the passport. No criminal records or terrorist watchlist checks are conducted using FR or any other biometric as part of CBP's Biometric Exit process.

CBP's present day biometric exit processing stems back to 1996, before there was a CBP or a Department of Homeland Security. It began with the passing of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA of September 30, 1996) which mandated that the INS use an automated system to record arrivals and departures (entry and exit) of non-U.S. citizens at all air, sea, and land ports of entry.

However, the IIRIRA did not include the collection of biometric identifiers for either entry or exit. That change occurred in the wake of the 9/11 terrorist attacks with the passing of the 2002 Enhanced Border Security and Visa Entry Reform Act (the "2002 Act"), an act that mandated biometric identification in addition to biographic identification for both entry *and* exit.[41]

After the homeland security reorganization of 2003, the newly created CBP assumed the frontline immigration functions of the former INS, along with the historic missions of the U.S. Customs Service and its post-9/11 counter-terrorism mission. Part of the creation of DHS included implementing biometric entry and exit as mandated by the 2002 Act; something the INS had not done.

As noted earlier, biometric entry was achieved by 2004. The U.S. was the first nation to do so, and it has significantly added to the security of the homeland. In response to the 2002 Act, with the assistance of DHS's US-VISIT program office,[42] in 2004 CBP began collecting biometric information

---

[41] CBP's authority to collect biometrics for both entry and exit was further codified with the passing of the 2004 Intelligence Reform and Terrorism Prevention Act as well as the 2007 Implementing Recommendations of the 9/11 Commission Act. Suffice it to say, Congress made it clear: they wanted biometrics taken on persons exiting the U.S.

[42] This program office was established by DHS for the purpose of designing, in coordination with CBP, a system to biometrically identify foreign nationals arriving at U.S. ports of entry.

from all foreign passengers, whether they were traveling with a State Department issued visa or under the Visa Waiver Program (VWP), as they arrived and before they were allowed to enter the U.S. The biometrics captured were finger scans at primary which were then run through IDENT (previously described) and the FBI's NGI, then known as NCIC. In 2004, there were roughly 30 million foreign passengers who arrived into the U.S. on commercial airlines. Pre-COVID, in 2019, that number increased to 40.4 million. In addition, a digitized photo was also taken. Thanks to US-VISIT, foreign nationals' fingerprints could be run with a red light, green light response within a few seconds. Not only was biometric entry important to protect against foreign terrorists entering the U.S., but it resulted in the arrest or denial of entry to many persons who were traveling under false identities, who were not the true visa holder, and a not insignificant number who had arrest warrants outstanding or were excludable because of prior criminal convictions or prior orders of deportation or removal. Indeed, in fiscal year 2019 alone, 288,523 foreign nationals were deemed inadmissible due, in part, to the existence of biometric entry.

With the implementation of biometric entry, that left the challenge of realizing the part of the 2002 Act requiring biometric *exit*. The US-VISIT program office was responsible for developing a workable biometric exit capability until circa 2013, when, as noted earlier, US-VISIT morphed into OBIM and the responsibility for biometric exit was re-assigned to CBP.

Although of far less importance to CBP's counter-terrorism mission, CBP, now tasked with this assignment, began to explore how to feasibly collect biometric identifiers as travelers exited the country. Indeed, CBP was directed by former DHS Secretary Janet Napolitano to explore potential biometric exit solutions that would carry out the longstanding Congressional mandate.[43] The issue of biometric exit received additional impetus with the issuance of the March 6, 2017 Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States," which required DHS to "expedite the completion and implementation of a biometric *entry [and] exit tracking system* for foreign travelers[44] to the United States." (Emphasis added). As noted, CBP has had a biometric *entry* system up and running since 2004. So, that left biometric *exit* begging for a solution.

One of CBP's missions is to administer and enforce U.S. immigration laws at our borders, including all of our nation's official ports of entry. Further, one aspect of effective control against illegal immigration, principally visa overstays, is accurately determining aliens who are lawfully present in the United States from those who have violated their terms of admission by overstaying. Without exit data, either biographic or biometric, it is difficult to determine whether foreign nationals have

---

[43] Thus, in addition to the repeated Congressional mandates of the 2002 Act and the 2007 Implementing Recommendations of the 9/11 Commission Act, CBP's efforts were also pursuant to 8 CFR § 215.8, "Requirements for Biometric Identifiers from Aliens on Departure from the United States," adopted on January 1, 2014. More specifically, this regulatory section provides that foreign nationals who depart the U.S. from a designated port of entry are "to provide fingerprints, photograph(s) or other specified biometric identifiers, documentation of his or her immigration status in the United States, and such other evidence as may be requested to determine the alien's identity and whether he or she has properly maintained his or her status while in the United States."

[44] The Regulation applies to non-exempt foreign travelers between the ages of 14 and 79.

overstayed their authorized periods of admission, or even how big a problem this is. A biometric confirmation of departure is reliable and marginally more accurate than relying only on biographic information regarding departures. The idea is that, if there is no evidence of exit within the period prescribed by a visa or the VWP's 90 days, that would be evidence that the alien is still in the U.S. and in the U.S. unlawfully. Unlike biometric *entry*, biometric *exit* has little to do with preventing terrorist attacks.

CBP collects *biographic* data on all travelers exiting U.S. international airports. This data is estimated to be accurate for approximately 98-99% of foreign travelers who entered under a visa (or the visa waiver program). Adding a biometric only marginally increases this already high percentage.

Neither CBP nor DHS has ever assessed that a biometric exit capability is needed for national security or counter-terrorism purposes. Moreover, even if a marginal case could be made for biometric exit, it has never been evaluated on a cost benefit basis. The fact is that this is not untypical for Congressionally mandated programs. This is important, because setting up a reverse U.S. VISIT infrastructure, *i.e*., exit infrastructure, at space-constricted U.S. international airports would be extraordinarily expensive and disruptive. That infrastructure already existed for biometric *entry* in the form of dedicated Federal Inspection Areas run by CBP at all U.S. international airports, but it does not exist for *exit*.

In an effort to comply with Congressional mandates, CBP's choice to pursue facial recognition[45] specifically, as opposed to any of the various other biometric modalities, was largely a consequence of an unavoidable reality. One of the chronic problems with the development of biometric exit, and unquestionably the reason it has taken so long, is that U.S. international airports, unlike Federal Inspection Areas on entry to these airports, are not, as previously mentioned, built to accommodate any type of immigration exit controls. The infrastructure does not exit to a reverse primary, including finger scans of the type implemented by CBP for entry back in 2004. Thus, if there was to be a biometric exit solution, CBP/DHS needed to develop a process that involved technological innovation which could be incorporated into existing airport infrastructure and was not overly disruptive to travel from the U.S. for both U.S. and non-U.S. citizens alike. Facial recognition was deemed the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy, and in a manner perceived as less invasive to the traveler (e.g., no actual physical contact is required to collect the biometric).

In coordination with, and support of, the commercial airlines and airport authorities, CBP rolled out its biometric exit solution beginning in 2017 to 2 U.S. airports. This process is now in place at 20 international airports in the U.S. In this process, travelers departing the U.S. via air, present themselves at a boarding gate operating biometric exit and have their photo captured by a camera connected to CBP's Traveler Verification Service (TVS) via a secure, encrypted connection. TVS then matches the

[45] As noted earlier, shortly afterward CBP implemented FR as the primary identifying biometric for Global Entry which further expedited an already fast process through the Federal Inspection Area for persons enrolled in in that Trusted Traveler program. As Global Entry is a voluntary program, this change from finger scans to FR has caused no controversy.

submitted photo with the existing photo templates held in the gallery for that flight via the NEC-3 algorithm. TVS then sends back a matching response (typically in less than one second) which informs next steps. If a match is found, the passenger proceeds to board the plane. If no match is found, airline personnel revert to their traditional practice of manually validating the traveler's identity by conducting a visual examination of their identity document (e.g., passport), and the traveler will then proceed to board the plane.

By way of background, in conjunction with one of the most accurate algorithms available today, CBP began operating its Traveler Verification Service (TVS) in 2017. The TVS is an accredited CBP information technology system that consists of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. As mentioned earlier, TVS builds "galleries" of photographs representing all the passengers on a manifest for a particular flight. These images may include photographs of non-U.S. citizens captured by CBP during a prior entry inspection, photographs from U.S. issued visas, U.S. passport photos and photographs from other DHS encounters.

As part of its rollout, CBP has taken significant steps to ensure data minimization and privacy protections by using an airline-generated alphanumeric Unique ID (UID) to disassociate the biographic information associated with the photo taken at the boarding gate. To further ensure privacy protections, CBP has implemented expansive opt-out provisions applicable to both U.S. citizens and aliens, posts information on those opt-out procedures near the point of collection, and per a recently released GAO report, those postings will be improved.[xvi] Further, photos of U.S. citizens, those who do not opt out, are retained for no more than 12 hours for continuity of operations purposes, and then deleted. For U.S. citizens, as has long been the case using biographic data, CBP retains only a confirmation of the outbound exit; nothing more than it has routinely done based on biographic information. The photos of non-U.S. citizens, and the associated encounter details, are securely transmitted to IDENT, which, as mentioned earlier, is the DHS-wide central repository for biometric and biographic information run by OBIM. Additionally, CBP does not allow its approved partners such as airlines and airport authorities to retain the photos for any length of time or purpose. These partners must immediately delete the photos once they have been sent to CBP for matching, and they must also allow CBP access to their systems for auditing purposes; another practice soon to be expanded as referenced in the aforementioned GAO report.

Further, CBP employs a face matching algorithm developed by the Japan-based company, NEC. As noted above, the NEC algorithm has consistently garnered high marks in NIST's FRVT for its accuracy. In NIST's December 2019 FRVT report on demographic effects in algorithms, it was noted that the algorithm currently employed by CBP (NEC-3) is, "on many measures, the most accurate we have evaluated." They also noted that, regarding the NEC-3 algorithm, as well as other top performers, "false positive differentials were undetectable."

The Subcommittee believes that CBP has come up with a creative and good solution to Congressionally mandated biometric exit. We believe it has appropriately addressed legitimate privacy

concerns of U.S. citizens through its opt out process.[46] But despite the benefits of biometric exit, and mainly because it was difficult logistically to separate out U.S. citizens, taking photos of outbound passengers as they depart the U.S. has raised concerns in Congress and among privacy NGOs. Much of the concern, based on our investigation, stems from misconceptions of how CBP is using FR for biometric exit. The push back in Congress and elsewhere against CBP's biometric exit solution appears to have caused consternation at the departmental level of DHS, with some thinking that CBP caught them off guard. What is clear is that the leadership of DHS and the DHS Policy Office may not have been as aware of the details of the biometric exit program as they would have liked. This internal misalignment and the fact that after the program rolled out CBP spent many hours explaining the program to Congress, the media and interested NGOs, reinforces the need for a communication and outreach plan at the front end before implementing a new biometric solution.

The Subcommittee's Recommendation No. 1 is designed to ensure awareness of and socialize new uses of technology at the department level, particularly potential new uses of controversial biometric technology, by requiring that an implementation plan be submitted to a Biometrics Oversight and Coordination Council (BOCC) chaired by the DHS Deputy Secretary. In Recommendation No. 8 we suggest that the proposing DHS operational component agency submit a communication and outreach plan concurrently with an implementation plan to the BOCC, *before* the widespread rollout of new biometrics or novel uses of existing biometrics. The BOCC will vet both the implementation and communication plans and, because both the Department's Privacy and CRCL offices will be represented on the Council, ensure that privacy concerns are appropriately addressed.

b. *Case Study No. 2: Opportunities to Leverage Biometrics between DHS Agencies*

The operational agencies of the DHS for the most part have significantly different missions that do not lend themselves to similar or overlapping programmatic solutions. They vary widely from traditional missions, such as the USCG's missions to protect fisheries and search and rescue on the high seas, to CBP's collection of duties and regulation of trade, to Secret Service's protection of the President. Even in the homeland security space, there is relatively little mission overlap.[47] There are, however, some similarities between the missions of some of the DHS agencies that provide the opportunity to leverage a program of one agency, including programs that use biometrics, with another DHS agency. One example is CBP and TSA, despite their vastly different authorities and often different approaches.[48]

---

[46] The airlines and airport authorities generally support the biometric exit program. It is they, not CBP, that for logistical reasons have resisted separate queues for U.S. citizens and foreign nationals.

[47] One example of overlap is prevention of maritime smuggling. USCG and CBP, through is Air & Marine Office, share responsibilities for protection in the territorial waters of the U.S. For the most part, with USCG having the lead role, this overlap has not been an issue.

[48] Since its creation in 2003, CBP has followed a risk management approach to screening and inspecting people and goods seeking to enter the U.S. TSA, largely because of Congressional mandate in the Transportation Security Act of 2001, is

The Joint CBP-TSA Project

As a result of CBP's efforts and successes in using facial recognition, CBP and TSA are participating in a joint pilot project. This pilot was first launched in March of 2017 at JFK International Airport to evaluate the use of facial recognition to automate identity verification at TSA checkpoints. The CBP/TSA pilot leveraged CBP's TVS for this purpose. As a traveler approached the TSA identity check process, rather than presenting an identity document for verification, a photo is taken by a CBP-owned camera. Like the CBP biometric exit process described above, the photo is then securely transmitted to TVS, and the matching response is returned. If a match is found, the traveler is directed to proceed onward through the TSA inspection process. If no match is found, the TSA officer would then revert to a traditional document check to verify the traveler's identity, and then the traveler would proceed onward. The pilot has now also been tested at Los Angeles International Airport (LAX) and is currently underway at Hartsfield Jackson International Airport (ATL) in Atlanta, Georgia. No photos taken as part of this identity verification process are stored by either TSA or CBP.

While the pilot has been largely successful in achieving its aims and is faster and more efficient at performing identity verification than either the CAT-C or CAT-2 process mentioned earlier, it is limited in that CBP only has access to manifest data for international flights. This means photos of domestic travelers are not added to the TVS galleries for matching purposes, which significantly limits those who are eligible for this facial recognition process only to international outbound travelers. Despite this, CBP and TSA are continuing to actively work together, and are presently planning to launch a new pilot where TSA will leverage TVS to automate the identity verification process for Trusted Travelers (e.g., both Global Entry and TSA PreCheck™ members) in dedicated checkpoint lanes. No launch date has yet been identified for this process, but there is optimism for its launch sometime in 2021. This could potentially eliminate the need for a TSA officer to perform a manual identity check for a significant segment of passengers who are Trusted Travelers.

The Subcommittee believes that such leveraging efforts, including their use of biometrics, are to be encouraged. Accordingly, one of the benefits our Recommendation No. 1, creating the Council, is that it will help ensure the sharing and discussion of successful uses of biometrics by one DHS agency and help identify the potential for leveraging those uses to support the missions of other DHS components.

required to do 100% screening of everyone seeking to board a commercial aircraft. To its credit, TSA has moved more toward risk management solutions in recent years.

c. Case Study No. 3: The Necessity of a Nimble Process

Because of potential privacy concerns, greater departmental oversight and coordination of biometrics is desirable. Nonetheless, DHS component agencies need latitude to initiate pilot programs that include biometrics in order to test whether they can play an effective role operationally. Often the "CONOPS" (concept of operations) is far more important than the technology. And the technology, no matter how good it is, is useless if it cannot fit into the CONOPS. Pilot programs allow the components to make this operational effectiveness determination without the need of first going through a cumbersome and time-consuming bureaucratic process prior to implementation. It is one reason we do not believe that establishing a headquarters level PMO (program management office)[49], even a PMO lite, over the uses of biometrics by DHS components is advisable.

But the need for nimbleness by DHS goes beyond pilot programs. There are truly new emergency situations faced by DHS components where the ability to move rapidly is essential. One such situation confronted CBP Border Patrol (CBP/BP) during the family unit migration crisis of 2019 where the need to collect DNA to establish claims of parentage was of the utmost importance, particularly when CBP/BP was being confronted with fraudulent claims of parentage by adult aliens who were illegally crossing the border with a "rent-a-child" from Central America. Meeting this child endangerment emergency head-on, ICE HSI, working with CBP/BP, pioneered the collecting and rapid analysis of DNA to protect tender aged children from exploitation.[50]

Traditional DNA testing has proven valuable for investigative purposes, both to prove guilt and innocence.[xvii] However, it requires shipping samples to the FBI lab, the results of which typically take days. This process is too time-consuming for persons apprehended by CBP/BP, where there is limited time to determine parentage and consider response options. Rapid DNA testing was developed, in part, by DHS S&T and allows DHS agents to run the DNA test while still in the field and have results for up to 7 different people at a time within 90 minutes.[51]

In the midst of the 2019 Family Unit Migration Crisis, when it became clear that some claims of parentage were false, CBP's Border Patrol (CBP/BP) initiated a new partnership with ICE Homeland Security Investigations (HSI), dubbed Operation Double Helix, whereby HSI agents collected DNA

---

[49] The DHS Policy Office advised the Subcommittee that its proposal for carrying out the Acting Secretary's January 2019 management directive, discussed in section IV of this Report, is for a PMO Lite, run by a program manager within the Policy Office, to provide DHS "governance" over all programs of DHS component agencies that use biometrics. For reasons discussed elsewhere, the Subcommittee believes this would be ill advised. In any event, given the structure of DHS, any requirement to seek approval of a program or a new use of biometrics by a DHS component agency should be at the S-2 level, as we recommend for the Council.

[50] DNA is the only biometric modality that can verify family associations, which makes it uniquely suited to assist several DHS component agencies' missions. USCIS also uses DNA test results as a means of confirming familial relationships for refugee and asylee processing when DNA testing appears warranted, though it cannot require it.

[51] Currently all familial verification DNA testing performed on persons apprehended by CBP/BP is voluntary and none of the DNA is stored (only the results of the test are kept).

for rapid DNA testing.[52] This testing is done to validate familial relationships and deter child exploitation schemes in which human smuggling organizations rent tender-age children to adults to help them gain entry into the U.S. There is evidence that the innocent victims of "rent-a-child" schemes were being returned to Central America and recycled.[53] Since the launch of a pilot program in May 2019, HSI has determined that approximately 11% of the adult aliens claiming to be parents, are not.[54] There is little question that moving quickly to DNA test those claiming to be a parent in order to gain release into the U.S. acted as a significant deterrent and reduced the number of children being used as pawns by human smuggling organizations.

One limitation on familial verification DNA testing, however, was that it could only be done on a voluntary basis. This limitation appears to have been removed by a final DOJ Rule titled "DNA-Sample Collection from Immigration Detainees" published in March 2020. This rule gives the Attorney General legal authority "to authorize and direct all relevant Federal agencies, including the Department of Homeland Security, to collect DNA samples from individuals who are arrested, facing charges, or convicted, and from non-United States persons who are detained under the authority of the United States." Under this DOJ Rule, it appears that, if authorized by the Attorney General, CBP/BP can now take DNA samples from aliens who have been apprehended illegally crossing the border with a child without obtaining the alien's consent, because under the rule such evidence "could be essential to the detection and solution of crimes [aliens] may have committed or may commit in the United States."[xviii]

As can be seen from the foregoing, there are times when DHS components must act rapidly, and this includes deploying new biometric capabilities. For this reason, the Subcommittee recommends that the departmental oversight structure allow for nimble and rapid implementation of new biometrics, for pilots *and* emergency situations. *See* Recommendation No. 2.

---

[52] This was recommended in the HSAC Final Emergency Interim Report from the CBP Families and Children Care Panel, p. 9, dated April 2019.

[53] Ibid., p. 7

[54] Where the alien claiming parentage is unrelated to the minor, federal prosecution is ordinarily sought for false statement to CBP, in addition to illegal entry.

V. Protection and Storage of Biometric Data

The Subcommittee examined how DHS stores and protects biometrics. As discussed in detail at in Section II.b above, across all of DHS, the central repository for biometric, and associated biographic data, is the Automated Biometric Identification System (IDENT). All component agencies of DHS that collect biometric data, store it in IDENT, which is operated and maintained by the Office of Biometric Identity Management (OBIM).

Since the launch of IDENT in 1994, there has been no evidence to indicate that any of its biometric and related non-biometric data has been compromised or exfiltrated. OBIM's success in protecting DHS' biometric data is achieved through rigorous process improvement in which OBIM works to reduce the risk of a data breach by evaluating all aspects of system operations. In instances of non-automated data sharing, when approved, OBIM shares data only with governmental entities. To further their protective measures, OBIM is presently working with DHS Headquarters to incorporate the Cybersecurity Infrastructure Security Agency's (CISA) Continuous Diagnostic and Mitigation Program to reduce cyber risk and provide visibility across all OBIM systems. This CISA program will incorporate a 72-hour vulnerability and remediation scanning process, asset protection, and security information and event management (SIEM).

Although most storage of biometrics is done by OBIM, and most accesses to biometric data is granted to direct-hired DHS employees, there are instances, usually associated with pilot projects, in which a contractor has access to biometrics and, under contract, is required to protect the data. While this process is largely carried out without issue, there are rare examples of errors which demonstrate the importance of punctiliousness regarding any such arrangements involving the private sector. One such example was part of CBP's Vehicle Face System (VFS) pilot which took place at the Anzalduas, Texas Port of Entry. A CBP subcontractor was hired to install their proprietary facial image capture solution and provide support for the associated equipment. While the CBP contractor was not responsible for the storage of the photos captured as part of the VFS pilot, it had access to them (albeit un-authorized access) while performing their maintenance work. And, although the contractor's employees were subject to strict data protection requirements and privacy protocols, and had undergone thorough background checks, had completed all CBP required training and had signed Rules of Behavior agreements, a breach still occurred. While performing maintenance on the cameras, on three separate occasions in 2018-2019, the contractor's employees downloaded a total of approximately 184,000 images from the system. Then, in 2019, the contractor's corporate network was subject to a ransomware attack that compromised thousands of those images (some of which were eventually published on the dark web). A review by the DHS Inspector General concluded that "CBP did not adequately safeguard sensitive data on an unencrypted device."[xix] The report provided key recommendations (to which CBP concurred) to help CBP address the vulnerabilities which led to this breach, however the incident itself highlights the importance of protecting biometric data across all mediums and in all storage capacities regardless of whether it is in transit or at rest.

We believe that protection of biometrics, particularly in association with biographic data, should be and is a priority for DHS. Accordingly, both the storage (duration) and protection of biometrics should

be part of implementation plans submitted by DHS component agencies for review by the DHS Biometrics Oversight and Coordination Council (BOCC), which includes CISA, a DHS agency with formidable expertise regarding the protection of data against hacking. Additionally, while our research turned up no examples indicating that the collection and storage of biometrics has caused issues, we believe, whenever possible, it is better to act in advance rather than to react.

Although not purely a process issue, the Subcommittee believes that DHS should consider setting forth clear policies reflecting the difference between biometrics used solely for identity matching (e.g., CAT-C/2 and TVS) and biometrics collected for investigative or background check purposes. Using the BOCC process we recommend DHS adopt such a two-tier approach. Indeed, biometrics for identity matching could be fast-tracked as outlined in Recommendation No. 2, below. Adopting this dichotomy may mitigate privacy concerns and, in our view, would reinforce guardrails against the misuse of biometrics.

VI. Sharing of Biometric Data Outside DHS

Once biometric information has been collected and stored, it can become a force multiplier when responsibly shared with the appropriate law enforcement and security partners via secure means. DHS shares its biometric data internally and with other federal agencies, as well as with U.S. state and local law enforcement agencies. Moreover, pursuant to agreements, almost always reciprocal, on a limited basis DHS shares biometric data with international partners also. In order to better understand how this works, while maintaining data security and upholding all applicable privacy laws, it is helpful to walk through the various layers one at a time, starting inside the U.S. government and working outward through state and local law enforcement to our international partners.

Preliminarily, it is worthwhile to consider what value sharing the data offers. While IDENT stores a tremendous amount of biometric data, it has its limitations based on the mission needs of the DHS components. On a localized scale, sharing data with, for instance, the FBI's NGI database offers both DHS and FBI access to more information to help achieve the mutually beneficial goals relevant to the missions of both. Beyond that, state and local law enforcement agencies have very limited biometric databases (if any) of their own to assist in their work. Forging sharing arrangements with those agencies enables them to more rapidly and effectively achieve their own mission goals, which promotes public safety and is potentially beneficial to every law-abiding person in this country. Further, sharing biometric data internationally assists the U.S., as well as our international law enforcement partners, in identifying transnational criminals, sex offenders, smugglers of humans and narcotics, gang members, terrorist and terrorism related information, fraud, and patterns of illegal migration.

Understanding the reasoning behind the sharing practices is important, but so too is understanding who negotiates these agreements and how they work. DHS' centralized biometric repository, IDENT, contains roughly 3.2 billion fingerprint images, 800 million facial images, and 3.5 million iris pairs.[55]

[55] This data is collected from, among others, visa applicants, border crossing encounters (both lawful and unlawful),

While OBIM is the steward of IDENT, and therefore the manager of how data is shared, the DHS Office of Policy, Strategy, and Plans (PLCY) is responsible for negotiating all biometric data sharing agreements with outside agencies on behalf of DHS and the DHS operational agencies. Also, as each agreement is unique and access is restricted, IDENT has been engineered with multiple filtering layers to allow different (and only agreed to) levels of access. Additionally, the records contained in IDENT are not "owned" by OBIM, a complicating factor for negotiating with agencies outside of DHS. Record ownership is maintained by the submitting organization (e.g., USSS, CBP, ICE, etc.), and they make the decision as to who can see their data. Needless to say, coordinating a department-wide position on sharing agreements has proven complicated and difficult, especially with international partners.

When DHS biometric data is shared with local and state law enforcement agencies, it is done through the DHS partnership and data sharing agreement with the Department of Justice (DOJ), FBI, and the interoperability between the IDENT and NGI systems. This is governed by the overall Memorandum of Understanding (MOU) between the DHS, DOJ/FBI, and the Department of State (DOS). That same MOU, as well as the MOU between DHS and the Department of Defense (DoD), also governs the vast majority of U.S. government interagency biometric data sharing.

As mentioned above, DHS not only shares biometric data with other U.S.-based agencies, it also engages in international biometric data sharing in support of operational missions, chiefly through the Migration Five Initiative, a Data Sharing Working Group comprised of Australia, Canada, New Zealand, the United Kingdom, and the United States. However, enabling biometric data sharing with other nations required a different kind of platform than the one used to share data within our borders. The Secure Real-Time Platform (SRTP), chosen by DHS/OBIM as its international information sharing architecture, is a mechanism for data sharing that is scalable to any country.[56] To support and manage SRTP, DHS has created the Biometric Data Sharing Program (BDSP) which is an identity data exchange solution that facilitates biometric and associated biographic information sharing between the U.S. and foreign partner nations.[57] The BDSP achieves a greater reach and further benefits by going so far as to build a host country's biometric system, interconnectivity for bilateral information sharing, and use of adaptable, modern, scalable technology for them. For example, these efforts recently led to DHS signed agreements with Guatemala, Honduras, and El Salvador to share biometric data.

DHS international data sharing is largely, but not exclusively, conducted through OBIM. ICE/HSI has 69 offices located in foreign countries, far more than any other DHS agency, and 8 Department of Defense liaisons in 51 countries. For decades, HSI attaché offices have been able to collect important

---

immigration violators, and credential applicants (e.g., Transportation Worker Identification Credentials [TWIC]).

[56] SRTP enables international partners to transmit and receive queries from IDENT via encrypted internet messages through the DHS gateway.

[57] The BDSP institutionalizes the collection of biometrics, such as fingerprint, face, and iris, as part of a sustainable and mutually beneficial identity management program for a trusted foreign partner nation.

investigative information from the host nation's law enforcement counterparts. The ability to be effective requires an ability to exchange information. In this vein, HSI created a program in 2011 called the Biometric Identification Transnational Migration Alert Program (BITMAP), briefly described earlier. BITMAP[58] was established to equip international partner-country law enforcement officers to collect and share biometric and biographic data on special interest individuals and to identify potential threat actors transiting through participating countries. Via BITMAP, ICE is able to track U.S. bound illegal migration patterns, take joint action with partner countries, and deter human smuggling through South and Central America. BITMAP has been credited with identifying several hundred known or suspected terrorists, in addition to criminals, drug smugglers, human traffickers, murderers, child predators and gangs like MS-13.

In order to accomplish this BITMAP data exchange process, foreign law enforcement partners electronically transmit enrollments using a one-way portal that goes directly to CBP for processing. Search and enrollments then automatically occur in the three primary USG biometric databases (IDENT, NGI, and the Department of Defense's Automated Biometric Identification System [ABIS]). Then, a consolidated biometric response is transmitted to in-country HSI personnel who oversee the BITMAP program. That official coordinates a response[59], if one is deemed necessary, back to the foreign partner.[60]

As may be evident, the international sharing of biometrics and other data has created issues of roles and responsibilities, including which component of DHS has the lead responsibility for entering into sharing arrangements with foreign partners. ICE/HSI, OBIM and PLCY all play roles, but the sharing of data truly requires a coordinated effort on behalf of the Department as a whole. For this reason, while reasonable minds may differ, the Subcommittee believes that the lead role in negotiating international agreements for sharing biometric data should be placed in PLCY. The lead role for executing such international agreements involving biometrics logically is OBIM in most situations. *See* Recommendation No. 7. Still, given its important overseas investigative role, HSI has strong equities regarding how these international agreements are negotiated and should be consulted and, indeed, should be a participant in the negotiations. Nonetheless, in this complicated arena, there have been tensions, and issues have arisen without a reasonably quick resolution process where, e.g., PLCY and HSI and/or OBIM do not see eye to eye. Creating a high-level Biometrics Oversight and Coordination Council (BOCC), as we have recommended, would provide a needed forum to help resolve these issues and recognize equities.

Binational biometric data sharing started as a means to better counter international terrorism. When done prudently and with adequate protections of the data exchanged, it can provide substantial benefits

---

[58] BITMAP is currently deployed to 18 countries.

[59] Using HSI's statutory authority for sharing information with foreign law enforcement under Title 19, USC Section 1628(a).

[60] All this is accomplished according to a communications plan that is established when BITMAP is set up with the foreign partners and stakeholders.

and improve the safety of the people of the U.S. and the world.

VII. Communication and Outreach: How DHS and its components communicate about Biometrics uses to the public and Congress

Informing Congress, the public, media and relevant stakeholders of new uses of biometrics is especially important, particularly as some uses, particularly FR, are controversial and raise privacy concerns.

With respect to biometrics, every component agency of DHS currently communicates their intent to launch a new program or develop a new system to the public in a variety of ways. Typically, this is done in the form of a Privacy Impact Assessment (PIA) or a System of Records Notice (SORN). Agencies must conduct a PIA to determine the privacy risks throughout the development life cycle of the program or system. PIAs contain general information on the reasoning for the program, details on how it will operate, the authorities underscoring its implementation, and any risks uncovered during the review process. PIAs, when complete, are published online at www.dhs.gov and some agencies also publish their PIAs on their own websites.

A system of records is a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. Once published, they are referred to as a System of Records Notice (SORN).

However, some agencies do not stop their communication efforts at PIAs and SORNs. Citizenship and Immigration Services (USCIS) also offers information on their public website regarding their biometric collection programs. Secret Service (USSS) posts privacy signage in the areas they are capturing biometric information. CBP/FO and the TSA post privacy signage (electronic and/or printed) and offer informational tear sheets/brochures at or near processing checkpoints where biometric programs are operating. They both also post information regarding their respective programs on their websites. Additionally, CBP publishes advertisements in travel related magazines, conducts regular meetings with private sector stakeholders to ensure they remain informed, and engages with the DHS Data Privacy and Integrity Advisory Committee (DPIAC) and the Privacy and Civil Liberties Oversight Board (PCLOB).

That said, there does not appear to be any mechanism within DHS for a departmental review and vetting of a DHS operational component's communication and outreach plan where the component agency is utilizing a new biometric in aid of one of its missions or a novel use of an existing biometric. Where use of a new biometric modality, or new use of an existing biometric modality, is being introduced, the Subcommittee believes that the responsible DHS component agency should do more than issue a PIA and, if appropriate, a SORN. It should have a thoughtful communication plan which outlines the purposes and limitations of the new use and which can, in turn, be used to brief Congress, the media and interested groups. This plan should be coordinated through the agency's public and congressional affairs offices, in coordination, as necessary, with the DHS public affairs and legislative

affairs offices.

The case study of biometric exit and the previously referenced GAO report both suggest that a communication and outreach plan be prepared in conjunction with the DHS component agency's implementation plan, and that both plans be reviewed by the departmental level Biometrics Oversight and Coordination Council (BOCC), as recommended by Recommendations Nos. 1 and 8.

VIII. Placement of OBIM

The Subcommittee sees no need for any major organizational restructuring of DHS to address the issues related to biometrics, with one exception: OBIM. OBIM started out as a Program Management Office (PMO) at a departmental level directorate, the Border and Transportation Directorate, which no longer exists. OBIM's current reporting relationship through the Under Secretary for Management strikes us as illogical and less than optimal, especially given its central role within DHS of storing and analyzing biometrics.[61]

In our experience, PMOs are usually intended to serve a critical start up function, but once its goals have been achieved, its functions are typically placed into the appropriate component(s) that most utilize the developed system. In the case of OBIM, formerly US-VISIT, it developed a biometric entry function using IDENT for CBP that was implemented in 2004. Despite achieving this goal, OBIM not only continued to receive and be the repository for biometrics, not just the fingerprints collected by the Border Patrol as part of the legacy INS program, IDENT, but also the vastly increased numbers of fingerprints generated by CBP via US-VISIT. Approximately 80-90% of the biometrics transactions involving OBIM are generated by CBP. Thus, one option is to devolve the functions of OBIM back to the operational agency of DHS that is by far the biggest collector and user of IDENT, that is, CBP. Another option is to maintain OBIM as a standalone entity but transfer and place it under CISA. Yet another possible option is to place it under PLCY. Given other issues involving the uses of biometrics, the Subcommittee did not study deeply the placement of OBIM and makes no consensus recommendation as to where it and its functions are optimally situated within the Department's organizational structure. Nonetheless, we believe this issue is worthy of a formal internal review by the Department.

[61] In February 2015 the Deputy's Management Action Group (DMAG) concluded that OBIM should be transferred, in its entirety, to CBP. See DMAG – Summary of Conclusions (Amended) February 10, 2015.

IX. Recommendations

The Subcommittee makes the following Recommendations:

The first six Recommendations are intended to respond to Taskings Nos. 1-3 of the seven taskings: (1) how DHS can establish a multi-year biometrics vision, strategy and implementation plan with performance metrics and oversight; (2) how it can establish clear roles and responsibilities within and between Department Components and Offices regarding the collection and use of biometrics; (3) best practices, if any, to create a biometric enterprise and governance process.

1. **Establish a DHS Biometrics Oversight and Coordination Council, with representation by the appropriate DHS agencies and offices. The Council would be chaired by the DHS Deputy Secretary.**

We recommend that DHS establish a Biometrics Oversight and Coordination Council (herein "Council" or "BOCC"). The Council will consider and, as needed, research and provide recommendations for all DHS policies regarding the use, collection, storage and sharing of biometrics. Based upon any written proposal or implementation plan endorsed and submitted by the senior officer of any DHS member of the Council, the Council members will assess, discuss and make recommendations regarding: (i) any new use by any DHS entity of any biometric tools or policies; and (ii) any use at DHS of new or pre-existing biometric technologies that have not previously been approved for DHS use.

Further, the Council will coordinate the use of biometric tools, data and operations among DHS agencies where there is an actual or potential operational overlap – or a clear need to coordinate investments and/or operational support among multiple DHS entities.

This internal departmental Council will include representatives at the component head from all DHS operating components, as currently defined; and the following departmental-level offices: Policy, OBIM, S&T, Privacy and CRCL. S-2 will establish a small secretariat to provide staff support to the Council.

Consensus among Council members is the optimal objective, but the Deputy Secretary shall (in consultation with the Secretary of Homeland Security, if necessary) have the clear authority to make final decisions for DHS regarding all matters that have been brought to the Council.

The Council shall meet quarterly – or at shorter intervals as necessary – to discharge its responsibilities as outlined herein. The formation of technical subcommittees for certain matters would likely assist the designated Council members with working at a faster pace. At least twice annually the Council shall devote an appropriate focus to assess the Department's overall success and challenges associated with DHS's use of existing biometric tools.

2. **The BOCC protocols should provide a fast-track process to approve pilots and emergency uses of biometrics, to include direct interaction between S-2, as Chair of the Council, and the relevant agency head.**

As discussed in the body of our report, the DHS must continue to have a nimble and proactive approach to use of biometric tools. DHS, through its operational components, has been a leader in making innovative and effective uses of biometrics. This progress has gone beyond traditional law enforcement uses of biometrics and is the direct result of innovation at the DHS component agency level. Thus, care should be taken not to stifle innovative uses of new biometrics where there are emergent threats or pilot projects to evaluate biometrics technologies and the operational protocols needed to support their use. For that reason, it is essential that there be a fast-track process for clearing pilot projects and emergency uses of new biometrics or existing biometrics in novel ways that do not involve convening the BOCC.

3. **The DHS Office of Policy should have the lead role within the Department regarding the development of biometric policies regarding biometric retention, privacy protection (in coordination with CRCL and PRIV), negotiating international agreements, and avoiding inappropriate bias.**

Although the Biometric Capabilities Executive Steering Committee (BC-ESC) has played an important role in coordinating department-wide approaches to biometrics uses and has also improved coordination, the BC-ESC, which has SES level representatives, is not a policy making body. Where department-wide policies are needed for biometrics, PLCY should have the lead in developing them. Where there is disagreement regarding a policy relating to biometrics, it should be elevated to the BOCC for resolution.

4. **The operational role for the collection and uses of biometrics should remain within the DHS agency that has the unique mission or program that is aided and/or made more effective with the use of biometrics.**

It would be a mistake to remove the operational role for collection and use of biometrics to an office at the DHS headquarters level, because divorcing such decision-making from the operational component is not advisable. Where more than one DHS agency is using the same biometric in support of the same type of mission, DHS, through the BOCC, should designate the lead agency for implementation, procurement, etc. and otherwise clarify roles and responsibilities, as necessary.

5. **Each DHS agency using biometrics shall designate one official within such agency with the responsibility for overseeing uses of biometrics for the agency.**

Some DHS operational agencies have one senior official knowledgeable and responsible for understanding the various ways and purposes for which the agency is using, or proposing to use, biometrics in aid of its mission. In our view, this is a best practice. There should be one official within each operational agency designated by the agency head that the agency head can look to in order to ensure, among other things, that implementation and communication/outreach plans are developed regarding proposed new uses of biometrics or novel uses of existing biometrics, for submission to the BOCC. The Agency Biometrics Official would also be responsible for engaging PRIV and CRCL, as appropriate, early in the process of development of such plans.

6. Update the Biometrics Strategic Framework of 2015

The DHS Biometric Strategic Framework (2015-2025) was, and still is, a useful document for articulating an overall departmental vision for biometrics moving forward. Importantly, it was developed through an intra-agency process. Since it was drafted five years ago, however, DHS operational agencies have increased their use of biometric modalities beyond finger scans, particularly to more controversial biometrics such as facial recognition. Given the pace of biometric development and increasing reliability, we believe it would be useful to update the Biometrics Strategic Framework every five years.

The following Recommendation is intended to respond to the 4th tasking: how DHS can establish consistency regarding how it shares biometrics with other federal, state, local, tribal and international law enforcement/security partners and with the private sector.

7. Where sharing of biometrics involves negotiations with other nations, DHS' Office of Policy should have the lead role, but the operational component(s) with equities and relationships should play an active role in negotiations.

There needs to be a lead negotiator for DHS regarding the bilateral or multilateral sharing of biometrics held by DHS. In our view, this role can be best executed by PLCY, which should solicit guidance from the BOCC, as necessary. Accordingly, PLCY should be designated the lead for negotiating international agreements regarding the sharing of DHS biometric holdings. OBIM should be designated as the lead that, when sharing is permitted, actually transmits or shares biometrics outside of the DHS.

DHS policy regarding sharing should be established, as needed, with inputs from the BOCC. Any DHS agency should have the discretion to propose a modification to DHS sharing policy to the Council, but PLCY should have the lead role in negotiating international sharing arrangements. Notwithstanding the foregoing, agencies of the DHS, such as ICE HSI, should continue to be permitted to share non-biometric information and intelligence outside of the DHS for law enforcement and security purposes. They may also share biometrics, provided they coordinate the sharing with and through PLCY. If there is disagreement at that level, any dispute should be promptly resolved by the BOCC.

Care should be taken to obtain input and participation from DHS agencies, such as ICE HSI, with equities in the sharing of biometric data and/or who have overseas offices dependent upon mutually cooperative relationships with host nation law enforcement.

The following Recommendation responds to Tasking No. 5: how can DHS better communicate with the public, Congress and stakeholders about how it intends to use and protect biometric information.

8. **In addition to an implementation plan, every new use of a biometric should require, concurrently therewith, a communication/outreach plan.**

Both plans should be simultaneously submitted to the BOCC. The communication plan will clearly address the purpose for which the new biometric will be used, the mission benefits from using the biometric, whether collection is voluntary, storage and retention planning, as well as what impact the proposed usage will have on privacy and civil liberties. If the implementation is approved by the BOCC, the communication plan will be used to communicate with and brief the media, Congress and stakeholders before or concurrent with implementation.

Recommendation Nos. 9 and 10 below is intended to respond to Tasking Nos. 6 and 7: (6) How can DHS improve its biometric collection, storage, matching, analysis and sharing capabilities, including uses of new and emerging biometric modalities to support DHS missions; (7) provide insight into how DHS can create a systematic and fully functioning Planning, Programming, Budgeting, and Execution (PPBE) process for biometrics.

9. **As part of its implementation plan, the DHS component agency proposing a new use of biometrics or a new biometric has the responsibility for evaluating and presenting the technical aspects, including matching and analysis, of the biometric and how it is to be integrated into operational protocols in support of the agency mission. The component agency or the BOCC should call upon S&T, as needed, to assist regarding the technical evaluation of the proposed biometric.**

The implementation plan, among other things, should provide the BOCC with information regarding the following on biometrics: whether they will be collected on a voluntary basis, whether biometrics will be collected on U.S. persons, whether the biometric is a 1:1 match or a 1:N match, OBIM's role, if any, and the storage protection and length of storage of biometrics collected by the DHS agency. As needed, S&T may be tasked by the BOCC, or by component agencies, to evaluate technical capabilities and biometric solutions to further a mission of the Department and/or one of its agencies.

Improving the Department's collection, storage, matching, analysis and sharing capabilities is fundamentally about assuring that the DHS has a robust, well-coordinated process to address these issues. Continuing to use the BC-ESC and establishing the BOCC should go a long way in achieving the desired improvements.

10. **The Management Directorate (MGMT), through its budget offices, should annually capture budget data related to different biometrics on an agency and department-wide basis and provide it to the BOCC to provide visibility to its oversight and coordination role.**

Generally, biometrics are part of programmatic budgeting and are not a separate line item. That said, the budget review process can be used more effectively to gain a broad understanding of the variety and kinds of biometrics collected and used by DHS' operational components. Accordingly, in addition to providing its budget coordination, MGMT should provide the BOCC with an annual budget analysis regarding agency and OBIM projected or requested expenditures for biometrics. This, in turn, will give the BOCC broad visibility across the Department and its operational agencies regarding not just the costs of biometric capabilities, but their usage.

APPENDIX 1: TASKING LETTER

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 21, 2020

MEMORANDUM FOR: Judge William Webster
Chair
Homeland Security Advisory Council

FROM: Chad F. Wolf
Acting Secretary, Department of Homeland Security

SUBJECT: **Four New Homeland Security Advisory Council (HSAC) Taskings**

Pursuant to the February 24, 2020 meeting of the Homeland Security Advisory Council, I am requesting that you establish four new HSAC subcommittees to undertake reviews of critical homeland security issues. The new subcommittees will be: (1) Economic Security; (2) Information and Communications Technology Risk Reduction; (3) Building Youth-Focused Engagements; and (4) Biometrics. An explanation and proposed scope for each subcommittee is listed below in items A through D.

Recommendations are due to the full Council no later than 180 days from the date of each subcommittee's formation. I would like an update and provisional findings from each subcommittee or panel at our next public meeting, which we will hold in early May 2020.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

D. Biometrics Subcommittee

The Biometrics Subcommittee will provide findings and recommendations on how the Department can implement a single and reliable approach to biometric identity management, both internally and with extremal partners. The subcommittee should examine the authorities, governance structures, and programmatic activities of the Office of Strategy, Policy, and Plans, (PLCY) and the Office of Biometric Identity Management (OBIM), with respect to developing and coordinating Department and government-wide policies, processes, and technical functions in support of DHS, Component, and the interagency. The subcommittee's mandate will include, but is not necessarily limited to, the following:

1. Provide recommendations on how the Department can establish a multi-year biometrics vision, strategy, and implementation plan with effective performance metrics and oversight.

2. Provide recommendations and best practices for the Department to establish clear roles and responsibilities within and between Departmental Components and Offices with respect to the collection and use of biometrics.

3. Provide recommendations and best practices for the Department to create a biometric enterprise governance and oversight process, while eliminating conflicting DHS biometric governance authorities and/or organizations.

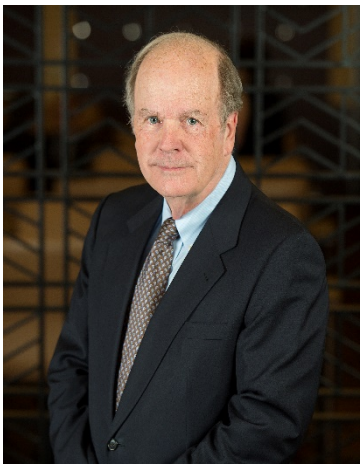
4. Provide recommendations on how the Department can establish consistency in how it accesses and shares biometrics with non-Departmental entities (e.g., private sector, state and local law enforcement, and federal, state, local, and tribal partners)?

5. Provide recommendations and identify best practices so the Department can clearly communicate with the public about how it intends to use and protect their biometric information.

6. Provide recommendations and identify best practices on how the Department can improve its biometric collection, storage, matching, analysis, and sharing capabilities, including using new biometric modalities and emerging matching technologies that have proven effective.

7. Analyze and provide insight into how the Department could create a systematic and fully functioning Planning, Programming, Budgeting, and Execution process for biometrics.

APPENDIX 2: SUBCOMMITTEE FOR BIOMETRICS BIOGRAPHIES



Robert Bonner
Principal, Bonner ADR & Consulting Services

Mr. Robert C. Bonner is a retired partner of Gibson, Dunn & Crutcher international law firm and formerly the senior principal of the Sentinel HS Group, LLC, a Washington, D.C.-based homeland security consulting firm. He is currently the principal of Bonner ADR & Consulting Services where he provides strategic advice regarding homeland and border security issues and serves as a neutral arbitrator and mediator in international disputes.

Mr. Bonner has held several positions in the federal government. In September 2001, he was appointed Commissioner of the U.S. Customs Service, and served until 2006 as the first Commissioner of U.S. Customs and Border Protection (CBP). Mr. Bonner is also a former Administrator of the U.S. Drug Enforcement Administration (DEA), U.S. District Judge and United States Attorney for the Central District of California. He was the chair of the California Commission on Judicial Performance and the Civilian Oversight Commission for the Los Angeles County Sheriff's Department. He currently serves on the board of trustees of the California Institute of Technology. Judge Bonner received a B.A. from the University of Maryland, College Park in 1963 and a J.D. from Georgetown University Law Center 1966.

Leon Fresco
Partner, Holland and Knight

Mr. Leon Fresco is an immigration attorney in Holland & Knight's Washington, D.C., office where he focuses his practice on providing global immigration representation to businesses and individuals. He also represents clients in administrative law and government relations matters and has extensive appellate, commercial litigation and legislation experience. Mr. Fresco was the primary drafter of S.744, the U.S. Senate's comprehensive immigration reform bill of 2013. He uses his broad range of experience to develop creative solutions to achieve his clients' objectives, which often may involve multi-stage representation before administrative agencies, federal courts and Congress.

Prior to joining Holland & Knight, Mr. Fresco was the Deputy Assistant Attorney General for the Office of Immigration Litigation at the U.S. Department of Justice (DOJ) Civil Division. In this position, Mr. Fresco provided litigation risk assessments to cabinet members in Executive Branch agencies. He also oversaw all civil immigration litigation on behalf of the federal government,

including representation of the DOJ, U.S. Department of Homeland Security (DHS), U.S. Department of Health and Human Services (HHS), U.S. Department of Labor (DOL) and U.S. Department of State (DOS).

Jayson P. Ahern
Principal and Head of Security Services, The Chertoff Group

Mr. Jayson 'Jay' Ahern is the Principal and Head of Security Services at The Chertoff Group. In this role, he advises clients on a broad range of issues including homeland and border security management, global commerce and supply chain security, critical infrastructure protection, risk management, and strategic planning/implementation.

Mr. Ahern served as a law enforcement professional for 33 years and as the former Acting Commissioner of U.S. Customs and Border Protection (CBP) at the U.S. Department of Homeland Security. As Acting Commissioner, Mr. Ahern was responsible for securing, managing, and controlling our nation's borders. With service in both domestic and foreign locations, he directed the agency's 58,000 employee workforce to keep terrorists and terrorist weapons out of the country, while also carrying out CBP's other border-related responsibilities.

Michael P. Jackson
President and Founder of Firebreak Partners

Mr. Michael P. Jackson is the President and Founder of Firebreak Partners, a company that provides specialized security and technology consulting services for critical infrastructure assets. On March 10, 2005, the U.S. Senate confirmed Mr. Jackson to serve as Deputy Secretary of the U.S. Department of Homeland Security (DHS).

Mr. Jackson served as DHS' chief operating officer, with the responsibility to manage the Department's day-to-day operations. Previously, Mr. Jackson served as Senior Vice President of AECOM Technology Corporation, where he was responsible for AECOM government relations globally and served as Chief Operating Officer of AECOM's Government Services Group. Mr. Jackson also served as Deputy Secretary of the U.S. Department of Transportation (DOT) from May 2001 to August 2003.

Hans C. Miller
CEO, Airside Mobile Inc.

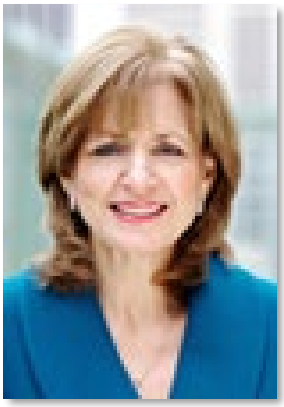
Mr. Hans C. Miller is the CEO and co-founder of Airside, a pioneer in the field of digital identity, privacy, and seamless travel. His work in aviation security has focused on security design, process flow, data analytics, and identity verification. With an emphasis on public-private partnerships, Mr. Miller has worked within or alongside the Departments of Homeland Security, Defense, Interior and Transportation to drive innovation.

Mr. Miller led the authorization and introduction of mobile boarding passes in the U.S. and helped co-write the global mobile boarding pass standard. In the aftermath of 9/11, he became the 11th employee of the nascent U.S. Transportation Security Administration (TSA), where he served in multiple senior executive roles and was awarded the Transportation 9-11 medal. Mr. Miller began his career at McKinsey & Company and has served as an adjunct faculty member at the Georgetown School of Foreign Service.

Chad Sweet
Co-Founder, The Chertoff Group

Mr. Chad Sweet is the co-founder & CEO of The Chertoff Group, a global advisory firm and investment bank exclusively focused on the security sector. Mr. Sweet advises companies and governments on their security and on mergers and acquisitions (M&A) in the security industry. With over a decade of investment banking experience, he has been involved in more than $5 billion of successful M&A and capital formation engagements.

Mr. Sweet was the former Chief of Staff of DHS and served in the CIA. He currently serves as Chairman of Trustwave Government Services, as well as a Director of the corporate boards of Coalfire and Salient CRGT. Finally, in the non-profit sector, he is a Senior Fellow at the George Washington Homeland Security Policy Institute, a Director on RAND's Global Center for Risk & Security, a Director of the Board of the Economic Club of Washington and a frequent commentator on security issues for FOX, CNN, CNBC and Bloomberg TV.



Karen Tandy
Former Administrator, Drug Enforcement Administration

Ms. Karen Tandy has more than 40 years of leadership experience in the public and private sectors with executive board experience serving on for-profit and nonprofit boards. Ms. Tandy heads a boutique government affairs consulting firm in the Washington D.C. area and is Executive Vice President of tele-health addiction recovery technology firm, NLW Partners.

During her public service, Ms. Tandy was appointed by President Bush and unanimously confirmed by the U.S. Senate as the first female to head the U.S. Drug Enforcement Administration (DEA). Before that, she served as U.S. Associate Deputy Attorney General during the Clinton and Bush Administrations, led the nationwide Organized Crime and Drug Enforcement Task Forces and served for 12 years as a federal prosecutor.

APPENDIX 3: BIOMETRIC MATRIX

	Biometrics-based Uses	**Biometrics** Being Collected	**Collection** Method	Using **Facial Recognition?**
USCIS	background checks, document production, identity verification	fingerprints, facial images, digital signature	fingerprint scanners, cameras, signature pad	No
USCG	background checks, identity verification	fingerprints, facial images	fingerprint scanners, cameras	No
CBP → **Field Ops**	Trusted Traveler vetting, Entry/Exit requirements, enforcement	fingerprints, facial images	fingerprint scanners, cameras	Yes
CBP → **Border Patrol**	arrests/booking	fingerprints, facial images, iris scans	fingerprint scanners, cameras, iris cameras	No
ICE → **HSI**	related investigatory uses such as forensic/ digital evidence, surveillance and arrests/booking	fingerprints, facial images, iris scans, voice file, DNA	fingerprint scanners, DNA collection kits, video and still cameras, iris cameras, recorders	Yes
ICE → **ERO**	arrests/booking, tracking while in ICE custody and under supervision, carrying out deportations	fingerprints, facial images, voice print, DNA	fingerprint scanners, cameras, DNA collection kits	No
TSA	Trusted Traveler vetting, credentialing, identity verification (limited pilot)	facial images, fingerprints	fingerprint scanners, cameras	Yes
USSS	arrest/booking, criminal investigations, applicant background checks, access controls	fingerprints, facial images, palm print, DNA, handwriting	fingerprint scanners, cameras, DNA collection kits	Yes

APPENDIX 4: SUBJECT MATTER EXPERTS

Name	Title	Agency/Organization
John Wagner	Deputy Executive Assistant Commissioner	CBP/FO
Courtney Ray	Director, Enforcement Systems Division	CBP/BP
Jason Thompson	Assistant Chief, Enforcement Systems Division	CBP/BP
Enrique Lucero	Executive Associate Director	ICE/ERO
Scott Kirby	Unit Chief, Data Driven Management Unit	ICE/ERO
Lee Bowes	Deputy Associate Director	USCIS
Matthew Allen	(A) Deputy Executive Associate Director	ICE/HSI
Hillary Hodge	Section Chief, BITMAP	ICE/HSI
Bart Cahill	Unit Chief, Identity and Benefit Fraud Unit	ICE/HSI
Jason Henry	Unit Chief, Law Enforcement Information Sharing Initiative	ICE/HSI
Meghann Peterlin	(A) Assistant Secretary, Office of Strategy, Policy, and Plans	DHS PLCY
Alex Zemek	Deputy Assistant Secretary, Office of Strategy, Policy, and Plans	DHS PLCY
Michael Scardaville	Principle Director and Senior Advisor, Information Sharing	DHS PLCY
Steve Yonkers	Director, Biometrics/Credentialing and REAL ID Program	DHS PLCY
Shonnie Lyon	Director	OBIM
Patrick Nemeth	Division Director, Identity Ops	OBIM
John Boyd	Assistant Director	OBIM
James Johnson	Director	DHS S&T
Arun Vemury	Program Manager	DHS S&T
Lauren Saadat	Director, International Privacy Policy	DHS PRIV
Dena Kozanas	Chief Privacy Officer	DHS PRIV
Peter Mina	Deputy Officer, Programs and Compliance	DHS CRCL
Brian Sterling	Section Chief, Security, Intelligence, and Information Policy Section	DHS CRCL
Ciaran O'Malley	Senior Advisor	DHS CRCL
Dan Boyd	Systems Engineer, Requirements Capabilities Analysis	TSA
John Latta	Deputy Assistant Administrator, Enrollment Services and Vetting Program	TSA
Jay Stanley	Senior Policy Analyst, Speech, Privacy, and Technology Project	ACLU
Jeramie Scott	Senior Counsel	EPIC
Lauren Beyer	Vice President of Security and Facilitation	A4A
Celine Canu	Head of Aviation Facilitation	IATA
Patrick Grother	Computer Scientist	NIST

APPENDIX 5: ADDITIONAL CASE STUDIES

The following two additional case studies are examples of the effective new use of biometrics within DHS; true success stories for which DHS can be justly proud.

a. Additional Case Study: Achieving Biometric Entry - - US-VISIT

As noted earlier in this report, in 2004 DHS established the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program to support the immigration, counterterrorism, and border security missions of CBP. US-VISIT provided the means for biometric identification of foreign nationals traveling to the U.S. The IDENT program (started by the Immigration and Naturalization Service in 1994), is a system for the storage and processing of biometric data and was assigned to US-VISIT shortly after the creation of DHS.

Under US-VISIT, starting in 2004, CBP began collecting fingerprints and a photo from arriving foreign nationals at all U.S. international airports. The fingerprints captured by CBP are run against the IDENT and NGI databases. IDENT, under US-VISIT's stewardship, has evolved into DHS' central repository for biometric data. IDENT's primary benefit was that it could link biometrics with biographic information to establish and verify identities. As of September 1, 2020, there are 267.1 million unique identities enrolled in IDENT, and since 2004 using IDENT on entry, CBP has identified numerous persons utilizing a false identity, been able to arrest a significant number of individuals who were wanted but were traveling under assumed names and/or fraudulent passports, and has also run all those fingerprints against the database of known or suspected terrorists, including, *e.g*., persons who traveled to Syria to fight for ISIS. These real-world successes using biometrics have disrupted criminals and adversaries from carrying out illicit activities in the U.S. and threatening American lives.

b. Additional Case Study: Global Entry - - An Effective Use of Biometrics

In 2005, CBP proposed to DHS a trusted traveler pilot program that became known as Global Entry. CBP recognized the potential for biometrics to perform its mission of facilitating legitimate travel and simultaneously improving their ability to secure the nation against further terrorist attacks. Global Entry was modeled on the already existing CBP land border trusted traveler programs, NEXUS, on the Canadian border, and SENTRI on our border with Mexico. To enroll in any of CBP's trusted traveler programs requires voluntarily providing biometrics and sitting for a personal interview by a CBP officer, among other things.

Global Entry was designed to make immigration and customs processing more efficient for vetted travelers by providing them a means of self-service immigration and expedited Customs processing; therefore, the more individuals who enrolled, the fewer the number of travelers CBP needed to scrutinize, *i.e.,* narrowing the haystack.

CBP officially launched the Global Entry program after securing approval from DHS in 2008. To

qualify for its significant benefits, applicants need to provide five years of their travel, employment, and residential address history. They also provide biographic information, pay a $100 application fee for a five-year enrollment ($20/year) and, as previously mentioned, sit for an in-person interview with a CBP officer at a GE enrollment center. If approved, GE members are able to utilize a kiosk without the need to stand in a queue to complete their U.S. immigration inspection. They also get expedited treatment through the Customs, or back end, of the Federal Inspection Area after retrieving their luggage. In this process, members would activate the kiosk by scanning their passport, and would then stand for a photo and provide fingerprints (4 fingers, either hand) to confirm their identity. They would then answer a short list of traditional customs declaration questions and confirm their flight details. Once complete, they receive a receipt and could bypass the rest of the immigration process, proceeding directly to baggage claim where they were also given a dedicated exit lane to ensure an expeditious customs inspection.

Global Entry proved to be enormously popular. Currently, there are 9.6 million individuals enrolled in Global Entry and its related trusted traveler programs. By FY2012, the Global Entry kiosks were processing 1.5 million travelers per year; however, the demand continued to grow, and by FY2019, the number of travelers being processed via the Global Entry kiosks had ballooned to almost 13 million per year. To address this growing demand and make the Global Entry kiosk transaction process even faster and more efficient, CBP began, in 2018, to pilot a program to incorporate facial recognition. Global Entry kiosks were modified so that the photo captured by the kiosk is used, in lieu of the fingerprint and passport scan, to verify the identity of Global Entry members. Facial recognition transactions have reduced kiosk processing time, already short, by an astonishing 90 percent. Since adding FR, over 2.4 million facial recognition kiosk transactions have been completed by Global Entry participants. The use of FR for Global Entry was initially piloted at Orlando International Airport (MCO), has now expanded to 19 airports as of August 2020 and CBP plans to continue its expansion of FR capability by adding 7 more airports before the end of the 2020 calendar year. FR has worked better than taking 4 finger scans, because approximately 2% of prints, particularly among elderly, are not readable, the capture process is faster, and it is touchless; a plus in times of pandemics, and further, is extremely accurate.

APPENDIX 6: GLOSSARY OF ACRONYMS

A4A – Airlines for America
AABB – American Association of Blood Banks
ABIS – Automated Biometric Identification System
ACLU – American Civil Liberties Union
ACRIMe – Alien Criminal Response Information Management
AFSP – Alien Flight Student Program
ARB – Acquisition Review Board
ATL – Hartsfield Jackson International Airport
BC-ESC – Biometric Capabilities – Executive Steering Committee
BDSP – Biometric Data Sharing Program
BITMAP – Biometric Identification Transnational Migrant Alert Program
BOCC – Biometrics Oversight and Coordination Council
BSC – Biometric Service Center
CART – Compliance Assistance Reporting Terminal
CAT – Credential Authentication Technology
CBP – U.S. Customs and Border Protection
CBP/AM – U.S. Customs and Border Protection/Air and Marine
CBP/BP – U.S. Customs and Border Protection/Border Patrol
CBP/FO – U.S. Customs and Border Protection/Field Operations
CEIU – Child Exploitation Investigations Unit
CFO – Chief Financial Officer
CFR – Code of Federal Regulations
CISA – Cybersecurity Infrastructure Security Agency
CODIS – Combined DNA Index System
CONOPS – Concept of Operations
CRCL – Civil Rights and Civil Liberties
DCA – Ronald Reagan Washington National Airport
DHS – Department of Homeland Security
DMAG – Deputy's Management Action Group
DNA – Deoxyribonucleic Acid
DoD – Department of Defense
DOJ – Department of Justice
DOS – Department of State
DPIAC – Data Privacy and Integrity Advisory Committee
EAGLE – Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement
EDDIE – EAGLE DirecteD Identification Environment
EPIC – Electronic Privacy Information Center
ERO – Enforcement and Removal Operations
FBI – Federal Bureau of Investigation
FEMA – Federal Emergency Management Agency
FP – Fingerprint

FPS – Federal Protective Service
FR – Facial Recognition
FRVT – Facial Recognition Vendor Test
FY – Fiscal Year
GAO – Government Accountability Office
GE – Global Entry
HART – Homeland Advanced Recognition Technology
HSAC – Homeland Security Advisory Council
HSI – Homeland Security Investigations
IAFIS – Automated Fingerprint Identification System
IATA – International Air Transport Association
ICE – Immigration and Customs Enforcement
IDENT – Automated Biometric Identification System
IIRIRA – Illegal Immigration Reform and Immigrant Responsibility Act
INS – Immigration and Naturalization Service
LAS – McCarran International Airport
LAX – Los Angeles International Airport
LEA – Law Enforcement Agency
LEO – Law Enforcement Officer
LEISI – Law Enforcement Information Sharing Initiative
LPR – Lawful Permanent Resident
MCO – Orlando International Airport
MGMT – Management Directorate
MOU – Memorandum of Understanding
NCIC – National Crime Information Center
NGI – Next Generation Identification
NGO – Non-Governmental Organization
NIST – National Institute for Standards and Technology
NPRM – Notice of Proposed Rule Making
OBIM – Office of Biometric Identity Management
OGC – Office of the General Counsel
OMB – Office of Management and Budget
OTCD – Operational Technology Cyber Division
PA&E – Program Analysis and Evaluation
PCLOB – Privacy and Civil Liberties Oversight Board
PIA – Privacy Impact Assessment
PII – Personally Identifiable Information
PLCY – Office of Policy
PMO – Program Management Office
POE – Port of Entry
PPBE – Planning, Programming, Budgeting, and Execution
PRIV – Office of Privacy

RDT&E – Research, Development, Test and Evaluation
S-1 – Secretary of Homeland Security
S-2 – Deputy Secretary of Homeland Security
S&T – Science and Technology
SES – Senior Executive Service
SIEM – Security Information and Event Management
SORN – System of Records Notice
SRTP – Secure Real Time Platform
TDC – Travel Document Checker
TSA – Transportation Security Administration
TSO – Transportation Security Officer
TVS – Traveler Verification Service
TWIC – Transportation Worker Identification Credentials
UID – Unique ID
USCG – United States Coast Guard
USCIS – United States Citizenship and Immigration Services
USSS – United States Secret Service
VFS – Vehicle Face System
VIP – Victim Identification Program
VWP – Visa Waiver Program

[i] Department of Homeland Security; *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338 (September 11, 2020).

[ii] Ross A.A., Jain A.K., Nandakumar K. *Introduction to Biometrics,* Springer, 2011, (Page 53).

[iii] National Commission on Terrorist Attacks Upon the United States (2004). *The 9/11 Commission Report.* New York: W.W. Norton & Company.

[iv] National Research Council 2010. *Biometric Recognition: Challenges and Opportunities*. Washington, DC: The National Academies Press. (Page 1).

[v] Corrigan, J. Legacy Systems Held DHS' Biometric Programs Back. Not Anymore., *Nextgov* (2019).

[vi] Kair, L. Biometrics can protect our borders – along with our privacy, *The Hill* (2019).

[vii] Schwartz, A. Mistakes, misuse, mission creep: Biometric screening must end, *The Hill* (2017)

[viii] Scott J.D. Facial recognition surveillance is here -- but privacy protections are not, *The Hill* (2017).

[ix] Grother, P., Ngan M., Hanaoka, K. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *National Institute of Standards and Technology* (Washington, D.C., December 19, 2019)

[x] Bushwick, S. How NIST Tested Facial Recognition Algorithms for Racial Bias, *Scientific American* (2019).

[xi] McLaughlin, M., Castro, D. The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist, *Information Technology & Innovation Foundation* (2020).

[xii] Burt, C. NEC tops several NIST Facial Recognition Vendor Test categories as accuracy at scale improves, *Biometric Update* (2019).

[xiii] Garvie, C., Frankle, J. Facial-Recognition Software Might Have a Racial Bias Problem, *The Atlantic* (2016).

[xiv] Warren, C. Unconscious Racism, *Psychology Today* (2020).

[xv] Bajak, F., Koenig D. Face scans for US citizens flying abroad stir privacy issues, *AP News* (2017).

[xvi] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO 20-568 (Washington, D.C., September 2, 2020).

[xvii] Butler J. M. (2015). The future of forensic DNA analysis. *Philosophical transactions of the Royal Society of London. Series B, Biological sciences*, *370*(1674), 20140252.

[xviii] Department of Justice; *DNA-Sample Collection from Immigration Detainees*, 85 Fed. Reg. 13483 (March 9, 2020).

[xix] OIG, *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot*, OIG-20-71 (Washington, D.C., September 21, 2020).