Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 27, 2020

Biometric Entry-Exit System: Legislative History and Status

The Department of Homeland Security (DHS) is statutorily required to develop and implement an automated biometric (i.e., physical characteristics such as fingerprints, face, or irises) entry-exit system for foreign nationals (referred to as *aliens* in immigration law) traveling into and out of the United States. The goals of this system are to strengthen national security and help enforce immigration law without disrupting the flow of authorized travel and commerce. The biometric entry system is said to be fully operationalized, whereas the biometric exit system is still being implemented.

Legislative History

Since mandating the development of an automated entry-exit system in 1996, Congress has amended the system's requirements and deadlines on several occasions, including by adding a biometric component in 2001. A timeline of related laws includes the following:

September 1996: The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA; P.L. 104-208), Section 110, required the Attorney General (AG) to develop an automated entry-exit system that would collect records of alien arrivals and departures by September 1998.

October 1998: Two appropriations acts (P.L. 105-259 and P.L. 105-277) amended Section 110 of IIRIRA to extend the deadline for implementing the entry-exit system to October 1998 for airports and to March 2001 for land and sea ports of entry (POEs).

June 2000: The Immigration and Naturalization Service Data Management Improvement Act of 2000 (P.L. 106-215) amended IIRIRA Section 110 to describe the entry-exit system in greater detail and imposed new deadlines of December 2003 for implementation of the entry-exit system at all U.S. airports and seaports, December 2004 for implementation at the 50 busiest land POEs as defined by the AG, and December 2005 for making data from the system available to immigration officers at all POEs.

October 2000: The Visa Waiver Permanent Program Act (P.L. 106-396), Section 205, required the AG to develop and implement a fully automated entry-exit system to collect arrival and departure records for travelers under the Visa Waiver Program at sea and air POEs by October 2001.

October 2001: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act; P.L. 107-56), Section 414, required the AG to implement the IIRIRA entry-exit system "with all deliberate speed." The act also directed the AG, in the development of the system, to focus on utilization of biometric technology and tamper-resistant documents. The law also required that the entry-exit system interface with certain law enforcement databases to identify individuals who may pose a threat to national security.

May 2002: The Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173), Section 302, required the AG, in developing the integrated entry-exit system at POEs, to use the technology standard under the PATRIOT Act, establish an arrival and departure database, and make all alien admissibility security databases interoperable (i.e., able to share data with other databases).

December 2004: The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Section 7208, required DHS (which was created in late 2002 and assumed responsibility for the nation's entry-exit system) to develop a plan to accelerate the full implementation of an automated biometric entry-exit system.

August 2007: The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), Section 711, required DHS to establish a biometric exit system to record the departure of all Visa Waiver Program air travelers by August 2008.

September 2008: The DHS Appropriations Act, 2009 (P.L. 110-329) withheld certain funding for the legacy United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program until DHS planned, piloted, and reported on a biometric air exit program.

December 2015: The Consolidated Appropriations Act, 2016 (P.L. 114-113) authorized fee increases on L-1 and H-1B visas to provide up to $1 billion dollars for DHS to implement a biometric exit system beginning in FY2017.

Executive Orders

The executive branch has also recently been involved in influencing the development of a biometric entry-exit system. Action by the Trump Administration includes the following:

March 2017: Executive Order 13780, Protecting the Nation from Foreign Terrorist Entry into the United States, ordered DHS to "expedite the completion and implementation of a biometric entry-exit tracking system."

Biometric Entry System

In December 2006, DHS fully implemented a biometric entry system for foreign nationals. It is part of the *primary inspection* at U.S. POEs. During primary inspection, U.S. Customs and Border Protection (CBP) officers conduct a brief interview with travelers, examine travel documents, and check travelers against the Interagency Border Inspection System (IBIS), a database of alleged and convicted criminals. Officers also conduct identity verification by entering some of the travelers' biographical (e.g., passport information) and biometric (e.g., finger scans and digital photographs) identification into the US-VISIT system. U.S. citizens are not required to provide biometrics upon entry to the United States.

Biometric Exit System

Unlike the entry system, the biometric exit system has yet to be fully operationalized. The Government Accountability Office (GAO) has periodically reported on the "various longstanding planning, infrastructure, and staffing challenges" to developing and implementing the biometric exit system. DHS, and then CBP (which took over the biometric entry-exit mission in 2013), piloted an array of programs using various biometric technologies (e.g., fingerprints, facial recognition, and iris scans). CBP determined that facial recognition technology (FRT) was the optimal approach because it can be performed relatively quickly and with a relatively high degree of accuracy (see "Accuracy," below). Its solution is called the Traveler Verification Service (TVS), which currently captures roughly 60% of *in-scope travelers* (i.e., foreign nationals aged 14-79) departing the United States via commercial air carriers. CBP's goal is to capture 97% of all in-scope departing commercial air travelers by 2022.

Traveler Verification Service

CBP, in partnership with the Transportation Security Administration, deploys TVS to verify travelers' identities utilizing FRT. TVS is a public-private partnership between the federal government and private airlines, airports, and cruise lines. CBP envisions that TVS "can replace manual checks of travel document across the travel continuum" at air, land, and sea POEs. TVS currently operates in 27 airports, 7 seaports, and 5 land border locations across the United States, as well as 4 preclearance locations.

A Matching Technology

TVS compares the travelers' *live photograph* (e.g., taken by a gate agent) to a gallery of photographs. The content of these comparison galleries depends on the travel context. For air and sea travelers, CBP uses biographic data (e.g., gender, date of birth, travel document type and number, nationality) obtained from flight and ship manifests via the Advance Passenger Information System (APIS) to gather all associated facial images from DHS holdings (e.g., photographs from U.S. passports, U.S. visas, CBP entry inspections, and other DHS encounters) into the gallery. For pedestrians and vehicle travelers, the gallery consists of photographs of frequent crossers at that POE. TVS provides a *match* or *no match* result within two seconds. In case of a no match, the traveler's identity is checked manually by an agent.

Accuracy

In contrast to other types of FRT that can provide numerous possible matches (e.g., FRT used by police to generate potential investigative leads), TVS is a binary (match or no match) technology. As such, TVS can produce two types of mistakes: false positives and false negatives. According to CBP internal analysis, TVS's false positive rate is .0103% (it did not report the false negative rate). The accuracy rate is affected by a number of factors, including the composition of the gallery against which a face is compared. Notably, the TVS galleries are relatively small because they are created for a specific flight, ship, or POE.

False matches pose potential security risks, as they may not flag a traveler using a false identity. False non-matches pose potentially less of a security risk, though they present unique challenges. In the event of a non-match, a traveler's identity is checked manually, and the technology's error can be corrected—although it could delay or disrupt travel.

A December 2019 National Institute of Science and Technology study found that FRT algorithms' accuracy rates can vary by demographic factors such as age, sex, and race. However, when examining TVS's accuracy, DHS reported that "CBP analysis found a negligible effect in regards to biometric matching based on citizenship, age, or gender." (CBP does not collect race/ethnicity data, so it uses citizenship as a proxy.)

U.S. Citizens' Ability to Opt-Out

U.S. citizens are allowed to opt-out of biometric exit participation and can instead undergo manual review of travel documents. CBP notifies travelers of this option through physical signs posted at POEs and verbal announcements. They also provide an FAQ sheet upon request. In addition, there is information about TVS on CBP's website. However, in a letter to DHS, discussed below, some policymakers expressed concern that CBP may not provide U.S. citizens with adequate notice about TVS or explain opt-out procedures clearly.

Data Retention and Security

CBP stores photographs of foreign nationals for 14 days in the Automated Targeting System (ATS) Unified Passenger Module (UPAX). After 14 days, photographs are transmitted to the Automated Biometric Identification System (IDENT), where they are retained for up to 75 years. In contrast, photographs of U.S. citizens are to be immediately deleted after the matching process. All photographs are to be purged from the TVS cloud after 12 hours, regardless of citizenship status.

During the July 2019 and February 2020 House Committee on Homeland Security hearings about DHS's use of FRT, many Members expressed concerns about data security and liability. In addition, on June 13, 2019, a few days after CBP announced a breach of data held by one of their subcontractors, over 20 House Members signed a letter to then-Acting DHS Secretary McAleenan expressing concern about CBP's use of FRT. Among other things, the letter inquired about the nature of the contracts with private partners, the legal liability of the private partners, and how CBP audits partner systems to ensure that they are purging the photographs consistent with aforementioned timelines.

Issues for Consideration

As the creation of a fully operational biometric entry-exit system has been mandated by Congress, policymakers may choose to conduct oversight over the speed and methods by which DHS and CBP continue to implement the system. Of particular interest may be the system's development timeline, concerns about the accuracy of FRT, and privacy issues related to the capture and retention of photographs.

Abigail F. Kolker, Analyst in Immigration Policy

IF11634

Disclaimer