Supporting Statement
Biometric Identity
1651-0138

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

In order to enhance national security, the Department of Homeland Security is developing a biometric based entry and exit system capable of improving the information resources available to immigration and border management decision-makers. These biometrics may include: digital fingerprint scans, facial images, iris images or other biometrics. Biometrics may be collected from travelers entering or exiting the United States. CBP continues to test and evaluate different technological and operational changes to improve the accuracy and speed of biometric collection.

The federal statutes that mandate DHS to create a biometric entry and exit system include: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337 (2000); Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396, 114 Stat. 1637, 1641 (2000); Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, 115 Stat. 272, 353 (2001); Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107-173, 116 Stat. 543, 552, (2002); Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, 118 Stat. 3638, 3817 (2004); Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266 (2007), Consolidated Appropriations Act, 2016, Public Law 114-113, 129 Stat. 2242, 2493 (2016), Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, 110 Stat. 3009-546 (1997), Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114-125, 130 Stat. 122, 199 (2015), and Sections 214, 215(a), 235(a), 262(a), 263(a) and 264(c) of the Immigration and Nationality Act of 1952, as amended, 8 U.S.C. 1184, 1185(a), 1225(a), 1302(a) (1303(a), 1304(c) and 1365b.

Proposed Changes: CBP is proposing to revise this collection of information to include the collection of biometrics from vehicles, this collection will not impose a time burden on the respondents and may reduce wait times at the ports of entry and exit.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

CBP will store and use biometric data from those aliens specified in 8 CFR 215.8 and 235.1. This information collected is used to provide assurance of identity, determine admissibility of those seeking entry into the United States, confirm exit from the United States for the purpose of tracking aliens who have overstayed their visa or are otherwise illegally present in the United States, prevent visa fraud, and identify known or suspected criminals or terrorists.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

CBP has deployed equipment and software so that CBP Officers can biometrically compare and authenticate travel documents that the Departments of State and Homeland Security issue to travelers arriving to or departing from the United States. Digital cameras are used to collect photos and digital fingerprint scanners collect fingerprint images from aliens seeking entry into the United States through our ports of entry, and digital cameras from travelers departing the United States.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

This information is not duplicated elsewhere. Government agencies that collects biometric information from non-US persons are: Department of State (DoS), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), Federal Bureau of Investigations (FBI-CJIS), Department of Defense (DoD).

However, these biometrics taken by other agencies are not collected at the ports of entry. CBP must collect biometrics from travelers to record entry and exit, and verify their identities (by comparing it to biometrics found in IDENT).

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize.

The collection of information does not have an impact on small businesses or other small entities.

6. Describe the consequence to Federal program or policy activities if the collection of information is not conducted, or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

It is crucial to border security decision makers and law enforcement officials that they have access to timely and accurate information on the biometric-based identification of individuals. Without this biometric information, there is an increased risk of mis-identifying non-citizens entering or exiting the United States or receiving other immigration benefits. Also, there is an increased risk that CBP, or other agencies, will not realize that an individual seeking entry or other immigration benefits poses a security risk or is an individual with an active want or warrant. DHS is under a statutory mandate to deploy a biometric entry/exit system pursuant to the statutes listed in (1) above.

7. Explain any special circumstances.

This information collection is conducted in a manner consistent with the guidelines in 5 CFR 1320.5(c)(2).

8. Federal Register Notice:

Public comments were solicited through two Federal Register notices dated May 25, 2018 (83 FR 24326) on which one comment has been received, and on August 9, 2018 (83 FR 39454) on which no comments have been received.

Comment Received: July 24, 2018
Comment from: Electronic Privacy Information Center, Marc Rotenberg, President
Comment:
CBP's Current Proposal to Collect Biometrics from Vehicles Fails to Provide the Public with Adequate Information about the Program

The Federal Register notice leaves many relevant questions unanswered about the implementation of the collection and the accuracy of the technology used. In-car facial recognition technology has more potential technical problems than regular facial recognition technology. The system must be able to distinguish windshield reflections from faces of passengers and detect the faces of passengers sitting in the backseat of the car who may be obscured. If people are wearing sunglasses, hats, or other headwear that an officer would normally ask them to remove before using facial recognition technology they would be unable to do so without stopping the car. There are also variations from the car that could cause errors, such as windshield tint. Additionally, passengers may not be looking up and toward the camera, so the image captured could be a profile or in-motion. Has CBP tested the facial recognition technology it intends to use under all of these conditions? What will CBP do if it cannot capture a clear image of all passengers while they are in their car?

It is not clear from the notice what databases CBP will use to compare to the facial scans captured at the border. CBP will run these scans against databases of visas and other travel documents of non-citizens, but will CBP also use databases of U.S. citizens? How does CBP plan to handle the fact that they will not know beforehand who is going to be crossing the border like they do at airports. What is CBP protocol if the facial scan does not match anyone in a citizen or alien database? How long does CBP plan to retain the biometrics collected from vehicles? Will the biometric data collected from vehicle scans be combined with data in license plate reader databases?

Implementing a Massive Facial Recognition Network Will Disproportionally Impact Marginalize Groups and Lead to Mission Creep

The use of facial recognition as part of the Biometric Entry/Exit program poses significant risks to privacy and civil liberties. The technology can be used on unsuspecting people from a distance in a covert manner and on a mass scale. Similarly, facial recognition can easily be applied to large amounts of pictures and videos posted online. Facial recognition gives the government the power to identify individuals whenever it wants and without the consent of the individual.

The implementation of a large-scale biometric surveillance network also runs a serious risk of mission creep. The program itself is built on mission creep as it takes photos handed over to the State Department for the explicit purpose of obtaining a passport and now uses the photos for a new biometric entry/exit program that leverages facial recognition. The probability of mission creep is heightened by the fact that there are few laws that regulate the collection, use, dissemination, and retention of biometric data.[21] As FOIA documents obtained by EPIC show and this Notice confirms, CBP envisions expanding the Biometric Entry/Exit program far beyond its current implementation at airports.

Ubiquitous identification eliminates an individual's ability to control their identities and poses specific risk to the First Amendment rights of free association and free expression. The agency will also assume specific obligations under the Privacy Act for the collection and use of this personal identifiable information. The use of facial recognition at the border has real consequences for U.S. citizens as well as non-U.S. citizens and will disproportionately impact marginalize groups.

Conclusion

EPIC recommends that CBP promptly conduct a public report analyzing whether there is an actual need for the program that justifies the privacy risks associated with the use of biometrics.

Specifically, the public report should address the possibility of using less privacy-invasive alternatives to biometric identification that will meet operational needs, including a cost-benefit analysis that contains a comparison of the likelihood and cost of a data breach between the Biometric Entry/Exit program and alternatives that do not use facial

recognition or other biometrics. Finally CBP should immediately suspend the implementation of the Biometric Entry/Exit program pending the results of the public report and until regulations are implemented by Congress providing appropriate safeguards for the use of biometrics.

CBP Program Response:

U.S. Customs and Border Protection (CBP) is working diligently to meet the Congressional mandate for Biometric Entry Exit in a way that is most efficient and secure for the traveler, and is the least disruptive for the travel industry while effectively enhancing immigration and border security. CBP updates its public website to include information about the biometric entry/exit program, including Frequently Asked Questions and Privacy Impact Assessments (PIAs). Many of the responses to the items in the public comment can be found using the information provided at www.cbp.gov/biometrics .

The CBP website and the various PIAs, readily available at www.dhs.gov /privacy, contain details on the current biometric exit process, including regulatory authorities, locations of technical demonstrations, and alternative procedures. In addition, CBP provides notices as required by the Privacy Act in the form of visible signs near the point of collection describing the photo capture and the alternative screening procedures. The signs may be either physical signs and/or electronic signs as well as verbal announcements to inform the public that CBP will be capturing the photos and that U.S. citizens may currently request alternative processing, in lieu of the biometric process. Specifically, a U.S. citizen may notify either the CBP officer or the airline-boarding agent that he or she would prefer alternative screening procedures and, instead may present credentials for manual identity verification using his or her travel document. If processes or procedures change, CBP updates these communications to ensure all outreach material is current and clear for the traveling public. CBP also continues to provide training to CBP Officer on biometric matching process as well as alternative screening procedures.

As discussed in the Traveler Verification Service (TVS) PIA, CBP transmits facial images of in scope travelers, pursuant to 8 CFR §§ 215.8 and 235.1, to the DHS Automated Biometric Identification System (IDENT) for retention as the traveler 's biometric encounter with CBP. The retention of photos in IDENT follows the IDENT retention schedules as outlined in the IDENT PIA. CBP is also sharing specified photos of in-scope travelers with the National Institute of Standards and Technology (NIST) under an interagency agreement to test technologies developed by specified vendors and to evaluate algoritlm1s on biometric projects. Photographs of non-U.S. citizens may also be retained in CBP's Automated Targeting System (ATS) Unified Passenger Module (UPAX) for up to 14 days for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. Photos of all travelers are stored in CBP's TVS cloud matching service for up to 12 hours for

continuity of operations purposes. For more information, see the *DHSINPPDIPIA-002 Automated Biometric Identification System (December 7, 2012)* and *DHS/ CBP/PJA-056 Traveler Verification Service (November 14, 2018),* available at www.dhs.gov/privacy.

The DHS Homeland Advanced Recognition Technology (HART) database is not operational. Prior to its deployment, PIAs and other announcements will be provided by the DHS Office of Biometric Identity Management (OBIM). Additionally, the facial images taken are not included in the data exchanged under the Preventing and Combating Serious Crime Agreements. For more information, see *DHS/All/PIA-064 Preventing and Combating Serious Crimes* (April 3, 201 8), available at www.dhs.gov/privacy.

As required by regulation, CBP continues to collect biographic and itinerary information from the airlines in advance of the flight in the Advanced Passenger Information System (APIS). Specifically, the APIS manifest consists of biographic information such as the name, date of birth, country of citizenship, passport information (number, country of issuance, and expiration date), and an airline-generated alphanumeric unique ID (UID). The manifest also includes specific details of the traveler's itinerary, such as flight number, carrier, originating airport, and destination airport. CBP has taken steps to promote data minimization and privacy protections by using this UID and other methods to disassociate the biographic information associated with the new facial images. In addition, fingerprints are collected under a separate procedure and are not associated with the facial images within the TVS facial matching process.

For U .S. citizens who voluntarily participate in the biometric process, CBP uses facial recognition technology to identify the traveler by comparing the traveler against his or her passport photograph or other photographs i n DHS holdings. CBP does not store facial images voluntarily collected from U.S. citizens under this initiative in IDENT, as U.S. citizens are not considered in-scope. Rather, photos of all travelers-including U.S. citizens-which are collected as a result of participating in this program, are retained in the TVS cloud matching service for up to 12 hours following verification of the traveler's identity for continuity of operations purposes. However, photos of U .S. citizens collected through this initiative are not stored in any other OHS system. For all travelers, including those U.S. citizens who voluntarily participate, CBP promotes data minimization and implements a privacy by design approach to include secure encryption, biometric templates, and alphanumeric unique identification.

For additional information on CBP's Biometric Entry-Exit Program, to include regulatory authorities, collection, storage and use of data, and compliance with the U.S. Department of Homeland Security's Fair Information Practice Principles (FIPPs), please visit the CBP website, www .CBP.gov, as well as the most recent TVS PIA, available at www. DHS.gov/privacy. As CBP continues to make progress on the development and implementation of a full biometric entry-exit system, CBP will continue to update its website and PIAs.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

There is no offer of a monetary or material value for this information collection.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

A SORN for DHS Automated Biometric Identification System (IDENT) June 5, 2007 (Volume 72, Page 31080) and a PIA for IDENT- DHS/CBP/PIA-012(a) August 9, 2017, a PIA for Biometric Exit Mobile Air Test- DHS/CBP/PIA-26 June 18, 2015, a PIA for Southwest Border Pedestrian Exit Field Test- DHS/CBP/PIA-027 March 5, 2018, will be included in this ICR. No assurances of confidentiality are provided.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

There are no questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

INFORMATION COLLECTION	TOTAL ANNUAL BURDEN HOURS	NO. OF RESPONDENTS	NO. OF RESPONSES PER RESPONDENT	TOTAL RESPONSES	TIME PER RESPONSE
Biometric Data, Fingerprint Modality	568,981	58,657,882	1	58,657,882	.0097 hours (35 seconds)
Facial/Iris Modality	136,355	54,542,118	1	54,542,118	.0025 hours (9 seconds)
Vehicle*	0	300,000	1	300,000	.0000
Total	705,336			113,500,000	

*Biometrics collected from vehicles will not require any physical response from those respondents and as such the time per response is zero.

Annual Public Cost

The estimated cost to the respondents is $33,221,326. This is based on the estimated burden hours (705,336) multiplied by (x) the average hourly wage rate for all-purpose air travelers ($47.10). CBP used the U.S. Department of Transportation's (DOT) recommended hourly value of travel time savings for intercity, all purpose travel by air

and high speed rail, which is provided in 2015 U.S. dollars. CBP assumes an annual growth rate of 0 percent; the 2015 U.S. dollar value is equal to the 2018 U.S. dollar value.[1]

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information.

There are no recordkeeping, capitalization or start-up costs associated with this collection.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing and support staff), and any other expense that would have been incurred without this collection of information.

The estimated annual cost to the Federal Government associated with the review of these records is $70,427,771. This is based on the number of responses that must be reviewed (113,500,000) multiplied by (x) the time burden to review and process each response (.0097 hours) = 1,100,950 hours multiplied by (x) the average hourly loaded rate for a CBP Officer ($63.97)[2] = $70,427,771.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of this Statement.

There has been a decrease in the estimated annual burden hours previously reported for this information collection due to compartmentalizing the modalities which have different time per response estimates. There was an increase in overall respondents as CBP has requested to revise this collection to include biometric collection from vehicles at no additional time burden.

16. For collection of information whose results will be published, outline plans for tabulation, and publication.

This information collection will not be published for statistical purposes.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

CBP will display the expiration date for OMB approval of this information collection.

---

[1] Source: U.S. Department of Transportation, Office of Transportation Policy. *The Value of Travel Time Savings: Departmental Guidance for Conducting Economic Evaluations Revision 2 (2016 Update)*, "Table 4 (Revision 2 - 2016 Update): Recommended Hourly Values of Travel Time Savings for Intercity, All-Purpose Travel by Air and High-Speed Rail." September 27, 2016. Available at https://www.transportation.gov/sites/dot.gov /files/docs/2016%20Revised%20Value%20of%20Travel%20Time%20Guidance.pdf. Accessed June 11, 2018.

[2] CBP bases this wage on the FY 2018 salary and benefits of the national average of CBP Officer positions, which is equal to a GS-12, Step 2. Source: Email correspondence with CBP's Office of Finance on June 1, 2018.

18. Explain each exception to the certification statement.

CBP does not request an exception to the certification of this information collection.

B. Collection of Information Employing Statistical Methods

No statistical methods were employed.