



DEPARTMENT OF HOMELAND SECURITY

8 CFR Parts 215 and 235

[Docket No. USCBP-2025-0033; CBP Dec. 25-06]

RIN 1651-AB12

Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States

AGENCY: U.S. Customs and Border Protection, DHS.

ACTION: Final rule with request for comments.

SUMMARY: This final rule amends Department of Homeland Security (DHS) regulations to provide that DHS may require all aliens to be photographed when entering or exiting the United States, and may require non-exempt aliens to provide other biometrics. The final rule also amends the regulations to remove the references to pilot programs and the port limitation to permit collection of biometrics from aliens departing from airports, land ports, seaports, or any other authorized point of departure. In addition, DHS is requesting comments on the specific collection process as well as costs and benefits for new transportation modalities.

DATES: *Effective Date:* This rule is effective on [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Submission of public comments: Comments must be submitted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may submit comments regarding the specific collection process as well as costs and benefits for the newly implemented transportation modalities (the Simplified Arrival process at air entry, sea entry processes, and the process for entry for

pedestrians at land) to the Federal eRulemaking Portal: <https://www.regulations.gov>.

Follow the instructions for sending comments.

Instructions: All submissions received must include the agency name and docket number USCBP-2020-0062 or RIN number 1651-AB12. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided. For detailed instructions on submitting comments, see the “Public Participation” heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Larry Panetta, Director, Biometrics Program Office, Office of Field Operations, U.S. Customs and Border Protection, by phone at (202) 344-1253 or via e-mail at larry.a.panetta@cbp.dhs.gov.

SUPPLEMENTARY INFORMATION:

Table of Contents

- I. Public Participation
- II. Executive Summary
 - A. Notice of Proposed Rulemaking
 - B. Background and Purpose of the Rule
 - C. Costs, Cost Savings, and Benefits
- III. Background
 - A. National Security and Immigration Benefits of a Biometric Entry-Exit Program
 - B. Facial Comparison-Based Entry-Exit Process Pursuant to this final rule
 - 1. Benefits of a Facial Comparison-Based Process
 - 2. Facial Comparison Technology Gallery Building

3. General Collection Process
4. Facial Comparison-Based Entry Process
5. Facial Comparison-Based Exit Process
6. Alternative Procedures and Public Notice
7. No Match Procedures
8. U.S. Nationals, Dual Nationals and Lawful Permanent Residents
9. Business Requirements for Public-Private Partnerships

IV. Summary of Changes to the Biometric Entry and Exit Regulations

- A. General Biometric Exit Requirement for Aliens
- B. Collection of Photographs from Aliens Upon Entry and Departure
- C. Collection of Biometrics When Departing the United States and Other

Minor Conforming and Editorial Changes

V. Discussion of Comments Submitted in Response to the NPRM

- A. Overview
- B. Discussion of Comments
 1. Comments Expressing General Support
 2. Comments Expressing General Support with Recommendations
 3. Comments Expressing General Inquiries
 4. Comments Expressing General Opposition

VI. Statutory and Regulatory Requirements

- A. Executive Orders 12866, 13563, and 14192
- B. Regulatory Flexibility Act
- C. Unfunded Mandates Reform Act of 1995
- D. Paperwork Reduction Act
- E. Privacy
- F. National Environmental Policy Act

Table of Abbreviations and Acronyms

ADIS—Arrival and Departure Information System

APA—Administrative Procedure Act

APIS—Advance Passenger Information System

CBP—U.S. Customs and Border Protection

DHS—Department of Homeland Security

DHS DPIAC—DHS Data Privacy and Integrity Advisory Committee

DHS TRIP—DHS Traveler Redress Inquiry Program

DHS FIPPS—DHS Fair Information Practice Principles

DOT—Department of Transportation

FBD—Facial Biometric Debarkation

FIS area —Federal Inspection Service area

FOIA—Freedom of Information Act

FY—Fiscal Year

GAO—Government Accountability Office

HART—Homeland Advanced Recognition Technology

IDENT—Automated Biometric Identification System

INA—Immigration and Nationality Act

LPR—lawful permanent resident

NARA—National Archives and Records Administration

NIST—National Institute of Standards and Technology

NPRM—Notice of Proposed Rulemaking

OBIM—Office of Biometric Identity Management

OMB—Office of Management and Budget

PIA—Privacy Impact Assessment

PII—personally identifiable information

PCLOB—Privacy and Civil Liberties Oversight Board

RFA—Regulatory Flexibility Analysis

SORN—System of Records Notice

S&T—Science and Technology

TSA—Transportation Security Administration

TVS—Traveler Verification Service

USCIS—United States Citizenship and Immigration Services

VWP—Visa Waiver Program

I. Public Participation

Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments on the specific collection process, as well as costs and benefits regarding the newly implemented transportation modalities for facial biometric collection, namely, the Simplified Arrival process at air entry, the sea entry processes, and the process for entry for pedestrians at land ports. Comments that will provide the most assistance will reference a specific portion of the final rule, explain the reason for any recommended change, and include data, information, or authority that supports such recommended change. All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided. Comments submitted regarding any topic other than the specific collection process and costs and benefits on these newly implemented transportation modalities are out of scope for this final rule and will not be considered.

II. Executive Summary

A. Notice of Proposed Rulemaking

On November 18, 2020, the Department of Homeland Security (DHS) published a Notice of Proposed Rulemaking in the *Federal Register* (85 FR 74162) (hereinafter

referenced as “the NPRM”) proposing to amend the DHS regulations with regard to collection of biometrics from aliens entering and exiting the United States.¹ On February 10, 2021, DHS published a notice in the *Federal Register* (86 FR 8878) stating that it was reopening the comment period for an additional 30 days based on comments received during the initial comment period.

DHS received a total of 320 comments in response to the NPRM. The submissions included comments supporting the rule, requesting clarification, providing suggestions for changes, and voicing concerns. After review of the comments, through this final rule, DHS is finalizing the proposed changes in the NPRM without substantive modification.

B. Background and Purpose of the Rule

DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics,² of

¹ The NPRM referred to “aliens” as “noncitizens.” This final rule uses the statutory term “alien” as appropriate.

² Biographic data includes information specific to an individual traveler such as name, date of birth, and travel document number, which are data elements stored in that traveler’s passport, visa, or lawful permanent resident card. Biometrics refers to forms of identification based on anatomical, physiological, and behavioral characteristics or other physical attributes unique to a person that can be collected, stored, and used to verify the identity of a person, e.g., fingerprints, photographs, iris, DNA, and voice print. *See* Executive Office of the President, National Science and Technology Council, Subcommittee on Biometrics, “The National Biometrics Challenge,” September 2011, available at <https://www.bing.com/ck/a?!&&p=e3dc11c7c1aa323eJmltdHM9MTcyOTIwOTYwMCZpZ3VpZD0zYmYzOTY1ZS01ZjU1LTU0YmItMTUzMC04MjJhNWUxYTY1MDQmaW5zaWQ9NTE5OA&pptn=3&ver=2&hsh=3&fclid=3bf3965e-5f55-64bb-1530-822a5e1a6504&psq=the+national+biometrics+challenge+2011&u=a1aHR0cHM6Ly9vYmFtYXdoaXRlaG91c2UuYXJjaGl2ZXMuZ292L3NpdGVzL2RlZmF1bHQvZmlsZXMuYmVlcm9zaXRlc9vc3RwL2Jpb2l1dHJpY3NjaGFsbGVuZ2UyMDEuLnBkZg&ntb=1>. (Last visited May 15, 2025.)

aliens entering and departing the United States.³ DHS also has broad authority to control alien travel and to inspect aliens under various provisions of the Immigration and Nationality Act of 1952, Pub. L. 82-414, 66 Stat. 163, as amended (INA), which may include requiring aliens to provide biometrics and other relevant identifying information upon entry to, or departure from, the United States.⁴ DHS, through U.S. Customs and Border Protection (CBP), has been collecting biometric data from certain aliens arriving in the United States since 2004.⁵ However, currently there is no comprehensive system in place to collect biometrics from aliens departing the country.

Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure helps address the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who remain in the United States beyond their period of authorized stay (overstays) or are present in the United States without being admitted or paroled, as well as incorrect or incomplete biographic data for travelers. As recognized by the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), combatting terrorism requires a screening system that examines individuals at multiple points within the travel

³ Numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data of aliens to verify their identity, and authenticates travel documents presented by such aliens through the comparison of biometrics. These include: section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. 104-828, 110 Stat. 3009-546, 3009-558; section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Pub. L. 106-215, 114 Stat. 337, 338; section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. 106-396, 114 Stat. 1637, 1641; section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56, 115 Stat. 272, 353; section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. 107-173, 116 Stat. 543, 552; section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638, 3817; section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Implementing Recommendations of the 9/11 Commission Act), Pub. L. 110-53, 121 Stat. 266, 338; and section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. 114-125, 130 Stat. 122, 199 (6 U.S.C. 211(c)(10)).

⁴ See INA 214, 215(a), 235(a), 262(a), 263(a), 264(c), 287(b) (8 U.S.C. 1184, 1185(a), 1225(a), 1302(a), 1303(a), 1304(c)), 1357(b)).

⁵ See the NPRM, 85 FR at 74169 for more information.

continuum.⁶ An integrated biometric entry-exit system provides an accurate way to verify an individual's identity, and, consequently, can improve security and effectively combat attempts by terrorists who use false travel documents to circumvent border checkpoints. An integrated biometric entry-exit system can also be used to biometrically verify that a person who presents a travel document is the true bearer of that document, which will help prevent visa fraud and the fraudulent use of legitimate travel documentation.

Such a system will also allow DHS to confirm more concretely the identity of aliens seeking entry or admission to the United States and to verify their departure from the United States. By having more accurate border crossing records of aliens, DHS can more effectively identify overstays and aliens who are, or were, present in the United States without being admitted or paroled and prevent their potential unlawful reentry into the United States. It will also make it more difficult for imposters to utilize other travelers' credentials. In addition, performing biometric identity verification can help DHS reconcile any errors or incomplete data in a traveler's biographic data.⁷ Ultimately, this provides DHS with more reliable information to verify identities and to strengthen its ability to identify criminals and known or suspected terrorists.

DHS has faced a number of logistical and operational challenges in developing and deploying a biometric exit capability. This is, in part, because U.S. ports generally do not have designated and secure exit areas for conducting outbound inspections, recording travelers' departures, or comparing biometric information against arrival data.

⁶ The 9/11 Commission Report 384-386 (2004), available at <https://9-11commission.gov/report/> (last visited May 15, 2025). *See also* the NPRM, 85 FR at 74107.

⁷ *See* the NPRM, 85 FR at 74107 for more information on how biometric identity verification mitigates risks including overstays, unlawful reentry, and other risks.

As stated in the NPRM, CBP has been testing various options to collect biometrics at entry and departure.⁸ The results of these tests and the recent advancement of new technologies, including facial comparison technology, have provided CBP with a model to implement a comprehensive biometric entry-exit solution. Based on these tests, CBP determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient.⁹ This technology uses existing advance passenger information along with photographs, which have already been provided by travelers to the U.S. government for the purpose of facilitating international travel, to create galleries of facial image templates to correspond with who is expected to be arriving in or departing from the United States on a particular flight, voyage, etc. These photographs may be derived from passport applications, visa applications, immigration applications, or interactions with CBP at a prior border inspection. Once the gallery is created based on the advance information, the facial comparison technology compares a template of a live photograph of the traveler to the gallery of facial image templates. Live photographs are taken where there is clear expectation that travelers will need to provide documentary evidence of their identity. If there is a facial image match, the traveler's identity has been verified. In select cases, fingerprints may also need to be collected, but only as required to better establish links to previously collected traveler biometric records.

CBP has fully implemented its facial comparison system in the commercial air environment at entry through a process known as Simplified Arrival. CBP has implemented exit in the air environment primarily through partnerships with airlines at select locations. CBP has also fully implemented facial comparison biometrics at entry in

⁸ See the NPRM, 85 FR at 74171-74173 for a discussion of these tests.

⁹ See the NPRM, 85 FR at 74173-74178 for a discussion of the benefits of a biometric entry-exit system based on facial recognition.

the sea environment through processes known as Facial Biometric Debarkation (FBD), Mobile Primary Face, and Simplified Arrival Sea, and at entry in the pedestrian land environment through a process known as Pedestrian Entry. CBP plans to eventually establish a biometric entry-exit system at all air, sea, and land ports of entry. *See* CBP, Biometrics, <https://www.cbp.gov/travel/biometrics> (last modified April 24, 2025) (last visited May 12, 2025).

As noted above, in this final rule, CBP is seeking comments regarding the specific collection process as well as costs and benefits for these newly implemented transportation modalities (the Simplified Arrival process at air entry, sea entry processes, and the process for entry for pedestrians at land).

CBP estimates that a biometric entry-exit system can be fully implemented at all commercial airports and sea ports for both entry and exit within the next three to five years. CBP plans to continue to work to determine the best option for implementing a comprehensive biometric entry-exit system nationwide, which may include pilot programs to test various options for travelers at exit in the sea and pedestrian land environment as well as for travelers entering and exiting in vehicles at land ports and on private aircraft.¹⁰ The regulatory changes adopted in this rule are necessary to enable CBP to continue its refinements, and implement facial comparison efficiently once the best solution is identified. As explained in the NPRM, prior to implementation of this rule, CBP could only conduct pilot programs at a limited number of air and sea ports of entry and could only collect biometrics from a limited population.

This final rule advances the legal framework for DHS collection and use of biometrics from aliens through a comprehensive biometric entry-exit system by removing

¹⁰ Private aircraft are those engaged in non-commercial flights, sometimes referred to as general aviation. *See* section 122.1(h) of title 19 of the Code of Federal Regulations (CFR) (19 CFR 122.1(h)).

the references to pilot programs and the port limitations and requiring facial comparison biometrics from all aliens on entry and exit. *See* 8 CFR 215.8(a) and 235.1(f). Because CBP is still determining the best way to implement biometric entry-exit in certain environments, as listed above, CBP has not included in this rule an analysis of the costs and benefits for those environments that are not yet operational. When CBP moves forward with a large-scale implementation of biometric entry-exit for vehicles at land ports and private aircraft or biometric exit at pedestrian land or sea ports, CBP will publish a notice in the *Federal Register* with information regarding details of implementation and request comments on the newly implemented transportation modalities.

This final rule provides that all aliens may be required to be photographed upon entry and/or departure. Facial comparison technology upon entry and departure makes the process for verifying aliens' identities more efficient and accurate. It enables CBP to match the travelers' biometric photographs with their biographic information. The ability to biometrically verify the identity to confirm the departure of aliens will improve security, comply with federal statutory requirements, and help DHS detect overstays and aliens who are or were present in the United States without being admitted or paroled and prevent their illegal reentry. Having accurate entry and exit records is a fundamental piece of the U.S. immigration system and detecting overstays supports that system. Remaining in the United States beyond the period of authorized stay is unlawful and carries consequences for future visits to the United States. *See* INA 212(a)(9)(B) (8 U.S.C. 1182(a)(9)(B)). Ensuring the travelers' photographs match with their vetted biographic and biometric information also helps CBP prevent document fraud and the use of fraudulent travel documents, or the use of legitimate travel documents by imposters (thereby also assisting in combatting identity theft), and to identify criminals and known or suspected terrorists.

CBP will comply with all legal requirements (e.g., the Privacy Act of 1974, 5 U.S.C. 552a (Privacy Act), section 208 of the E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899, 2921 (44 U.S.C. 3501 note) (E-Government Act), and section 222 of the Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, as amended (Homeland Security Act) (6 U.S.C. 142)) and departmental and government-wide policies that govern the collection, use, maintenance, and disposition of personally identifiable information (PII), including biometrics. As discussed in section III.B.6 of this final rule, U.S. citizens¹¹ may voluntarily participate in the biometric verification process. To minimize the data collected on U.S. citizens, CBP will not retain photographs of U.S. citizens collected as part of CBP's biometric verification program in CBP databases once CBP verifies that a traveler is a U.S. citizen. Encounter photos of U.S. citizens will be used exclusively for identity verification purposes and any photos of U.S. citizens will be discarded within 12 hours of verification of the individual's identity and citizenship.

C. Costs, Cost Savings, and Benefits

CBP anticipates that during the time period of analysis (2017–2029) this final rule will result in costs, cost savings, and benefits to CBP, approved partners, and travelers. CBP estimates total costs to CBP, outbound air travelers, inbound pedestrian travelers, and approved partners will range between \$1.3 billion (in discounted 2024 U.S. dollars) using a three percent discount rate and \$993 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized costs are estimated to be between \$122 million using a three percent discount rate and \$119 million using a seven percent discount rate. Meanwhile, total cost savings to inbound air and sea travelers, and CBP,

¹¹ For the purposes of opt out and photo retention policies, U.S. non-citizen nationals are treated the same as U.S. citizens.

will be between \$578 million (in discounted 2024 U.S. dollars) using a three percent discount rate and \$406 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized total cost savings are estimated to range between \$54 million using a three percent discount rate, to \$49 million using a seven percent discount rate. Total net costs from the implementation of this final rule are expected to range between \$722 million (in discounted 2024 U.S. dollars) using a three percent discount rate to \$587 million (in discounted 2024 U.S. dollars) using a seven percent discount rate. Annualized net costs are estimated to range between \$68 million using a three percent discount rate and \$70 million using a seven percent discount rate.¹²

Additionally, some travelers may perceive having their photographs taken for facial comparison as a loss of privacy; however, CBP could not quantify these costs. Other cost savings that CBP was unable to monetize were an estimated time savings to vessel carriers from a swifter debarkation process when using Facial Biometric Debarkation, approximately 1.25 hours per vessel arrival. Improving national and homeland security efforts through the application of facial comparison technology during biometric identification of individuals entering and leaving the United States is the primary benefit of this final rule. CBP was unable to quantify these enhanced security benefits. Table 1 below shows CBP’s estimates for future annualized costs, costs savings, benefits, and net costs from this final rule using three and seven percent discount rates over the period of analysis (2017–2029).

Table 1. Estimated Annualized Cost, Cost Savings, Benefits (2017–2029) (discounted thousands of 2024 U.S. dollars)

	3% Discount Rate	7% Discount Rate
--	------------------	------------------

¹² In the economic analysis for this final rule, CBP used a 3% and 7% discount rate showing values in discounted 2024 U.S. dollars, for estimated future quantified and monetized costs, costs savings and benefits.

Costs		
Annualized monetized costs	\$122,259	\$118,870
Annualized quantified, but not monetized costs	None	None
Qualitative (non-quantified) costs	Perceived privacy loss	Perceived privacy loss
Cost Savings		
Annualized monetized cost savings	\$54,355	\$48,599
Annualized quantified, but not monetized cost savings	None	None
Qualitative (non-quantified) cost savings	None	None
Benefits		
Annualized monetized benefits	None	None
Annualized quantified, but not monetized benefits	None	None
Qualitative (non-quantified) benefits	Enhanced National Security and identification of visa overstays	Enhanced National Security and identification of visa overstays
	Once fully implemented possible shorter plane turnaround times	Once fully implemented possible shorter plane turnaround times
Net Costs Annualized	\$67,904	\$70,271

III. Background

As discussed above, CBP is responsible for implementing an integrated, automated entry-exit system that matches the biographic data and biometrics of aliens entering and departing the United States. Furthermore, to carry out its mission responsibilities to control the border and to regulate the arrival and departure of both U.S. citizens and aliens, CBP has the authority to confirm the identity of all travelers and verify that they are the authorized bearers of their travel documents. *See* INA 287(b) (8 U.S.C. 1357(b)).

A. National Security, Public Safety, and Immigration Benefits of a Biometric Entry-Exit Program

The primary benefit of a biometric entry-exit system is the enhanced security provided by having biometric confirmation of the identification of alien travelers entering and leaving the United States. CBP has a comprehensive automated biographic information-based system that vets and checks aliens entering and departing the United States. Although this information is extremely valuable to CBP in completing its mission, no biographic information-based system, by itself, can definitively verify the identity of persons presenting travel and identity documents. Modern e-passports can make passport fraud more difficult. However, the best tool to combat passport fraud is to utilize the digital photos contained in e-passports to biometrically verify that a person who presents a travel document is the true bearer of that document. CBP's biometric tests using facial comparison technology support this conclusion.¹³ DHS expects that the implementation of this rule will greatly enhance DHS's ability to identify more of these imposters.

In addition to the benefits this technology can provide on entry, an integrated system, including biometric exit, is also essential for maintaining the integrity of the U.S. immigration system. Under current statutes and regulations, entering or staying in the United States without official permission from the U.S. government can cause a person to be legally barred from reentry to the United States for a number of years following that person's departure or removal.¹⁴ The absence of an effective biometric exit process has enabled aliens who are present in the United States without being admitted or paroled or who overstayed their authorized period of admission (overstays) to evade immigration

¹³ See the NPRM, 85 FR at 74167-74169 for more discussion on how e-passports mitigate fraud.

¹⁴ See INA 212(a)(9)(B) and 217(a)(7) (8 U.S.C. 1182(a)(9)(B) and 8 U.S.C. 1187(a)(7)); see also 8 CFR 217.4(a).

laws and avoid the time bars associated with unlawful presence. For Fiscal Year (FY) 2022, DHS estimates that about 853,955 aliens who entered by air or sea and were expected to depart that year overstayed their lawful period of admission, or 3.67 percent of aliens arriving by air and sea.¹⁵ Through its deployment of biometric exit pilots, CBP has been able to process and document hundreds of aliens who were present in the United States without being admitted or paroled.¹⁶ Additionally, biometric exit verification can allow CBP to address errors that sometimes appear in an alien's biographic data.

Finally, a comprehensive and integrated biometric entry-exit system serves as an important tool in the fight against global terrorism. Since the 9/11 attacks, the United States remains vulnerable to the threat of global terrorism. Recognizing terrorism as one of the most serious threats to international peace and security and the need to take immediate action to address the evolving threat environment, the United Nations Security Council adopted a resolution on December 21, 2017, calling on member nations to increase aviation security and to develop and implement systems to collect biometric data to properly identify terrorists.¹⁷ The resolution was co-sponsored by 66 countries, including the United States, and passed the Security Council with unanimous support. CBP's biometric exit program will provide another layer of identity verification and another opportunity to stop these individuals from departing without opportunity for further investigation.

¹⁵ DHS, FY 2023 Entry/Exit Overstay Report (2024), https://www.dhs.gov/sites/default/files/2024-10/24_1011_CBP-Entry-Exit-Overstay-Report-FY23-Data.pdf (last visited May 15, 2025).

¹⁶ See generally Enterprise Management Information System-Enterprise Data Warehouse (internal CBP reporting system); and CBP, DHS/CBP/PIA-034, Privacy Impact Assessment for the Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW) Appendix A (2016 and subsequent updates), available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp_emis_edw-appendixd-january2021.pdf (last visited May 15, 2025).

¹⁷ S.C. Res. 2396 (Dec. 21, 2017), available at <https://www.un.org/securitycouncil/content/sres23962017#:~:text=Decides%20that%20Member%20States%20shall,and%20suspected%20terrorists%2C%20including%20FTFs> (last visited May 15, 2025).

CBP has conducted extensive tests of the biometric comparison technology prior to implementation of this final rule. All of those tests support CBP's statements above regarding the efficacy of the congressionally mandated biometric entry-exit process.¹⁸

B. Facial Comparison-Based Entry-Exit Process Pursuant to this final rule

In this final rule, DHS is amending the regulations to provide that all aliens may be required to be photographed upon entry and departure from the United States. *See* 8 CFR 215.8(a), and 235.1(f). Failure to comply with a requirement to be photographed may result in a determination of inadmissibility or a violation of the terms of the alien's status where CBP requires this information to determine identity or other immigration information.¹⁹

Facial comparison technology will provide DHS a successful foundation for a biometric exit solution, as well as an improved and more streamlined biometric entry process. The following sections discuss CBP's facial comparison-based entry-exit process pursuant to this final rule. This process has been implemented for entry and exit at commercial airports and for entry at sea ports and pedestrian land ports. In this final rule, CBP seeks comments on these newly implemented transportation modalities. CBP will proceed with full implementation of an entry-exit process at all land modalities and for private aircraft, as well as on exit at sea ports, after refining its biometric exit strategies in those environments. Additionally, when CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea

¹⁸ *See* the NPRM, 85 FR at 74171 -74173 for more discussion regarding CBP's prior biometric comparison tests and the results of those tests; *see also* CBP, Biometrics, <https://www.cbp.gov/travel/biometrics> (last modified Apr. 16, 2025) (last visited May 1, 2025).

¹⁹ *See* 8 CFR 215.8(b) and 8 CFR 235.1(f)(1)(iv). In the event of technical failures preventing the capture and matching of photographs of travelers at entry or exit, air carriers and CBP officers will be directed to use manual boarding processes until the systems are functional. In this scenario, a biographic travel record will be created for the traveler but a biometric confirmation will not exist. A missing biometric confirmation record based on technology or operational failures is not considered non-compliance with the regulatory requirements.

ports, CBP will publish a notice in the *Federal Register* providing information regarding details of implementation in each new environment and request comments on the newly implemented transportation modalities.

Some of the facial comparison-based entry and exit processes described below may already be implemented in limited form at entry or under biometric exit pilot programs. For such existing processes, CBP adheres to all applicable laws and regulations that govern its collection of biometrics. Pursuant to this final rule, CBP may collect and compare facial images under the processes described here from all aliens arriving in and departing from the United States.

1. Benefits of a Facial Comparison-Based Process

CBP has developed a model for implementing a biometric entry-exit solution using facial comparison technology, currently implemented at commercial air entry and exit, pedestrian entry, and sea entry. As fingerprint scans have proven to be an effective law enforcement tool, CBP will continue to capture fingerprints as one of the initial identification biometrics at entry to the United States.²⁰ However, CBP has determined that facial comparison technology is currently the best available method for biometric verification at entry and exit as it is efficient, accurate, and unobtrusive. CBP may elect not to collect fingerprints for subsequent identity verification (after collecting them during the initial encounter) where CBP has implemented facial comparison.²¹ Fingerprint scans can be used for most aliens should facial comparison fail to properly identify the traveler.

²⁰ Note that the U.S. Department of State also collects biometrics from visa applicants and U.S. Citizenship and Immigration Services (USCIS) collects biometrics at other times that may be accessed by CBP as well.

²¹ CBP may collect facial images from all aliens entering or exiting pursuant to this rule, and, when requested, aliens must comply with CBP requirements to submit facial biometrics. CBP also has discretion not to collect facial images in certain cases where CBP determines that is appropriate.

The key benefit of using facial comparison for biometric identity verification (as opposed to fingerprints) is its efficiency. The facial comparison process leverages information that all travelers provide to the U.S. government as a condition for international travel. In general, photographs of travelers are readily available to DHS through sources such as previous encounter photos and visa databases, eliminating the need to collect new information and add another layer to the travel process. In addition, a system that matches a traveler's facial biometrics against a limited number of stored photographs, rather than an entire government database of photographs, significantly reduces the amount of time necessary to verify a traveler's identity. As a result, CBP is able to verify the identity of arriving or departing travelers with a high degree of efficiency while facilitating travel for the public.

Biometric verification using facial comparison is highly accurate. The National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Demographic Effects Report (NIST FRVT Demographic Effects Report) shows that facial comparison technology is able to match travelers at a rate of greater than 98 percent.²² If the system fails to match a traveler, then a manual review of the traveler's document is performed. Although CBP does not intend to cause delay or adverse consequences for the traveler in these situations, CBP is aware that in rare cases, travelers who fail to match are referred to secondary inspection or to a CBP officer for additional inspection, which may delay or hinder travel.

As an added benefit, a biometric entry-exit system based on facial comparison is relatively unobtrusive. It relies on current traveler behaviors and expectations; most travelers are familiar with cameras and do not need to learn how to have a photograph

²² See NIST, NISTIR 8280, FRVT Part 3: Demographic Effects 8, 26 (2019) (NIST FRVT Demographic Effects Report), available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf> (last visited May 15, 2025).

taken. Finally, the biometric capture device can be installed at an airline departure gate without any necessary changes to existing airport infrastructure.

By collecting photographs from all aliens departing the United States, DHS can more effectively verify their identity and confirm their departure. It also helps DHS identify known or suspected terrorists or criminals traveling using someone else's documents before they depart the country. This collection also helps identify visa overstays and aliens who are present in the United States without having been admitted or paroled, and prevent their illegal reentry into the United States, as well as prevent visa fraud and the use of fraudulent travel documents. After confirmation that the traveler is not the true bearer of a presented travel document, the traveler would then be subject to further inspection, first by the airline and also in some circumstances by CBP officers, which may include fingerprinting and/or an interview. Through this additional inspection, CBP will be better able to identify known criminals and other threats to border security.

The collection of photographs from all aliens avoids the need to have different processes at the point of departure for different alien travelers depending on whether they are exempt or not (such as the exemption based on age provided by the regulations prior to the effective date of this final rule). Collecting photographs from all alien travelers aligns with international passport standards, which require a photograph of the traveler on the document regardless of age or visa classification.

DHS has also determined that the collection of photographs from all aliens at entry is necessary, without regard to age, visa classification, or immigration status. Establishing a requirement that all aliens may be photographed without exemption enables DHS to biometrically verify the identity of all alien travelers traveling to and from the United States, thereby helping prevent visa fraud and the fraudulent use of legitimate travel documentation.

Collecting photographs from all aliens at entry also enables CBP to implement a streamlined entry process using facial comparison for all such aliens. For example, under the Simplified Arrival process, CBP primarily uses photographs rather than fingerprints to verify the traveler's identity and retrieve the traveler's biographic information for inspection.²³ Facial comparison technology can perform the function of biometrically verifying an alien traveler's identity much more efficiently than collecting and comparing an individual's fingerprints each time a person enters and exits the United States.²⁴ The Simplified Arrival process (which applies only to certain in-scope aliens prior to the effective date of this final rule and will thereafter apply to all aliens) utilizes integrated biometric identity verification with the retrieval of a traveler's biographic data from a single capture of a photograph. In doing so, the Simplified Arrival process eliminates the need for CBP to scan a passport or travel document to pull up the traveler's biographic data for inspection because a facial comparison scan performs this same function more quickly. Using facial comparison at entry can eliminate several administrative processes that will ultimately increase the speed at which CBP can inspect travelers arriving in the United States. By eliminating the administrative tasks involved in scanning a travel document or collecting fingerprints, CBP can devote more resources to interviewing an alien traveler to determine the person's admissibility. The increased efficiency benefits travelers by allowing them more time to make airline connections and spend less time waiting in lines to be processed by CBP. The increased efficiency also benefits the travel industry by allowing faster processing of customers which decreases resources required to process customers as well as increasing customer satisfaction.

²³ See the NPRM, 85 FR at 74173 for more discussion on the Simplified Arrival process.

²⁴ Note that CBP will continue to collect fingerprints during initial encounters with aliens entering the United States.

Pursuant to this rule, DHS may collect photographs from all aliens seeking to enter or exit the United States regardless of their age for the purposes of identity verification. This enables DHS to associate the immigration records created for children to their adult records later, which will help combat the trafficking of children, and screen for criminal history or associations with terrorist or other organizations seeking to violate applicable law throughout a person's lifetime. The exemptions in the current regulations for biometric collection based on the age of the individual (i.e., under 14 and over 79) were based on technological limitations on collecting fingerprints from children and elderly persons, as well as traditional law enforcement policies and other policies, such as not running criminal history background checks on children. These exemptions are not applicable to CBP's facial comparison-based biometric entry-exit program, as the use of biometrics has expanded beyond criminal history background checks and now plays a vital role in identity verification and management, and combatting the trafficking of children. Furthermore, internal CBP studies of biometric facial match accuracy, historical matching data, examination of biometric matching of ages under 14 and over 79, and CBP standard operating procedures associated with these ages no longer support exempting facial biometric collection from these populations. Exemptions based on age will continue to apply to biometrics other than facial images.

Certain privacy advocates have expressed concern over the accuracy of facial matching technology especially as it relates to demographics such as age, race and sex. CBP has conducted extensive testing of facial matching technology and CBP's internal analysis shows that facial comparison technology as used in international traveler screening operations is able to match travelers at a rate of greater than 98 percent. By expanding the scope of individuals subject to facial image collection, more travelers can be successfully matched. This will improve the experience for all segments of the

population, including children and the elderly.²⁵ Additionally, removing biometric exemptions for aliens alleviates the need to have multiple processing procedures for aliens, which would be a resource-intensive process. For entry and exit at land ports and for private aircraft as well as for exit at sea ports, CBP plans to continue to refine biometric exit strategies with the ultimate goal of implementing a comprehensive biometric entry-exit system nationwide. The regulatory changes in this final rule support CBP's efforts to regularly conduct a variety of statistical tests to bolster performance thresholds and minimize any possible bias impact on travelers of a certain race, gender, or nationality.

In this final rule, CBP has not analyzed the costs and benefits for implementing a facial comparison-based biometric entry-exit program for vehicles at land ports and private aircraft, or for exit at sea ports and pedestrians at land ports because CBP is still in the process of determining the best way to implement biometric entry-exit within each of these unique environments.

2. Facial Comparison Technology Gallery Building

CBP has developed a matching service for all biometric entry and exit operations that use facial comparison, regardless of the method of entry or exit (i.e., air, land, and sea) known as Traveler Verification Service (TVS). For all biometric matching deployments, TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a "gallery." These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, immigration applications, and photographs from other U.S. government encounters. CBP builds galleries of photographs based on where and when a

²⁵ See Nat'l Inst. Standards & Tech. (NIST), NISTIR 8271, Face Recognition Vendor Test (FRVT) Part 2: Identification 9 (2019), available at <https://doi.org/10.6028/NIST.IR.8271> (last visited May 25, 2025).

traveler will enter or exit. If CBP has access to Advance Passenger Information System (APIS) manifest information, CBP will build galleries of photographs based on upcoming flight, vessel, or, in some cases, bus arrivals or departures. If CBP does not have access to APIS manifest information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP may build galleries using photographs of aliens that frequently cross for that specific port of entry, taken at that specific port, that become part of a localized photographic gallery. CBP's TVS facial matching service then generates a biometric template for each gallery photograph that is stored in the TVS virtual private cloud for matching when the traveler arrives or departs.

3. General Collection Process

Due to the complexities in logistics and variety of air, land, and sea port designs across the entry and exit environments, CBP will collect photographs of the arriving or departing traveler via several different methods depending on the local port of entry and mode of travel. Generally, when travelers present themselves for entry or exit, they will encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection. This camera matches live images with existing photo templates from previously submitted passenger travel documents or other photos that CBP possesses (e.g., CBP encounter photos). The camera may be owned by CBP, the airport or air or vessel carrier, another U.S. government agency such as the Transportation Security Administration (TSA), or a foreign commercial partner. Once the camera captures a quality image and the system successfully finds a match among the historical photo templates of all travelers from the gallery associated with that particular manifest or port, the traveler proceeds to inspection for an admissibility determination by a CBP officer or is permitted to depart the United States. When a no match occurs, CBP or the carrier may use an alternative means to verify the traveler's identity, such as use of

an alternate biometric modality like fingerprints, or a manual review of the travel document as has been done historically.

4. Facial Comparison-Based Entry Process

Historically, prior to admission of a person to the United States, CBP used a manual process to inspect travel documents, such as passports or visas, to initiate system checks and verify a traveler's identity, travel history, and any law or border enforcement concerns that may require attention. The new primary entry solutions, including Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry, use biometrics to initiate the transaction and system checks, using facial comparison as the primary biometric verification modality. This shift from a biographic, document-based system to a biometric-initiated transaction requires travelers to provide facial photos for identity verification purposes. This enables CBP to more accurately verify identity and citizenship by matching the traveler's photograph with vetted and validated biographic information that is associated with a validated photo. Studies show that humans can benefit in face comparison tasks when assisted by a machine, and vice versa.²⁶

At entry, CBP uses CBP-owned cameras, CBP's primary arrival subsystem of TECS (not an acronym), and the TVS facial matching service to capture facial biometric data from travelers seeking to enter the United States. TVS automatically creates a template from the image and uses the template to query against a gallery of known identities, based on the manifests for entering flights and vessels that day. At this time,

²⁶ See P. Jonathon Phillips, et al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, 115 PNAS 6171 (2018), <https://www.pnas.org/content/pnas/115/24/6171.full.pdf> (last visited May 15, 2025). See also Hamood M. Alenezi & Markus Bindemann, The Effect of Feedback on Face-Matching Accuracy, 27 Applied Cognitive Psych. 735 (2013), <https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.2968> (last visited May 15, 2025); and Matthew C. Fysh & Markus Bindemann, Effects of time pressure and time passage on face-matching accuracy, 4 Royal Soc'y Open Sci. 170249 (2017), <https://royalsocietypublishing.org/doi/full/10.1098/rsos.170249#RSOS170249C16> (last visited May 15, 2025).

CBP is not actively using galleries of known travelers in the land vehicle environment. CBP uses gallery matching in some instances at land borders, such as bus manifest processing. The process works the same as in the air and sea environments, but APIS submission is currently voluntary for commercial bus and rail operators. CBP does not receive a manifest for pedestrians crossing the land border on foot or for persons traveling in private vehicles. CBP is conducting technical demonstrations to determine the feasibility of gallery matching in the personal vehicle environment at entry. CBP uses one-to-one matching in environments where no manifest exists, such as pedestrian entry. In those cases, CBP will use facial comparison technology to compare the live image captured at the time of application for entry with the traveler's travel document (e.g., passport) when possible.

5. Facial Comparison-Based Exit Process

CBP is using biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders. These partnerships enable CBP to more effectively verify the identities of individuals entering and exiting the United States, identify aliens who are violating the terms of their admission, and expedite immediate action when such violations are identified. In some partnership arrangements, an airline or airport authority partner uses its own technology and staff to incorporate TVS biometric facial comparison during the boarding process. These stakeholders have to adhere to strict business requirements and the cameras must meet CBP's technical specifications to capture facial images of travelers, prior to use. Each camera is connected to the TVS via a secure, encrypted connection.

During the boarding process, CBP's facial comparison matching service allows CBP to biometrically verify the identity of travelers departing the United States with the assistance of airline or airport partnerships. Once the traveler's photo is captured via a camera at the departure gate, TVS generates a template from the departure photo and uses

that template to search the gallery of historical photo templates in the cloud-based gallery. Some airlines now accept CBP's biometric identity verification in lieu of boarding passes as part of a new paperless, self-boarding process. Carriers, pursuant to the APIS regulations, are responsible for comparing the travel document to validate the information provided and ensure that the person presenting the document "is the person to whom the travel document was issued." 19 CFR 122.49a, 122.49b, 122.75a, and 122.75b. The use of TVS provides a more efficient and accurate way to meet this requirement.

Typically, on air exit, CBP is not permanently stationed at the gate. Therefore, CBP currently relies on the review of biographic data (provided via APIS) to determine whether further inspection on departure is warranted and whether an outbound enforcement team should be sent to the gate. With the use of facial comparison technology, outbound enforcement teams are informed immediately when a no match occurs (via notification on a mobile device) and may, in some cases, determine that additional inspection is warranted. The carrier may also notify CBP if additional CBP inspection is needed.

Outbound processing for travelers on commercial sea vessels (e.g., cruise ships) will resemble the air exit process. It is expected that this process will also be based on an APIS traveler manifest, although CBP is still determining the best way to implement this process. CBP may collect biometrics from travelers leaving the United States at land borders, when staffing permits. CBP may consider and examine partnering opportunities in the future in the land environment to enable more complete collection of biometrics at exit at land borders. When CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea ports, CBP will publish a notice in the *Federal Register* providing information regarding details of implementation

in each new environment and request comments on the newly implemented transportation modalities.

6. Alternative Procedures and Public Notices

All U.S. citizens and nationals are subject to inspection upon arrival into and departure from the United States to confirm their identity and citizenship. *See* INA 287(b) (8 U.S.C. 1357(b)). However, where CBP has implemented a biometric verification program, participation by U.S. citizens in the biometric verification process is voluntary. A U.S. citizen traveler who does not wish to have a photograph taken may request an alternative inspection process. U.S. citizens may notify the airline or vessel boarding agent or a CBP officer if they would like to opt out of the facial comparison-based process at the time of boarding or during the entry process and request that an alternative method of validation be employed. The citizen's identity will then be verified manually by CBP or the gate agent examining the travel document. For example, in the event a U.S. citizen elects not to be photographed at airports where CBP is conducting biometric exit verification, an airline gate agent should perform a manual review of the U.S. citizen's passport. Although CBP and carriers make every effort to ensure no delays or adverse consequences result when a U.S. citizen opts out of the biometric collection, CBP is aware that in some cases, U.S. citizens have alleged that they have been referred to secondary inspection or told they would not be able to board because they declined biometrics. Individuals who feel they were unduly delayed and would like further information regarding their travel record may request information about records contained in the CBP systems through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) online at <https://www.dhs.gov/foia-contactinformation>.

CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII, as set forth in this rulemaking, the CBP biometrics website regarding CBP's Biometric Privacy Policy, <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>, the TVS Privacy Impact Assessment (PIA),²⁷ and the CBP Privacy Office report entitled "CBP Privacy Evaluation (CPE) of the TVS in support of the CBP Biometric Entry-Exit Program" (CPE TVS Report).²⁸ As detailed in the CPE TVS Report, when airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP.²⁹ CBP provides notice to travelers at the designated ports of entry through both physical and either electronic message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP will be taking photos for identity verification purposes. CBP also provides notice to the public that a U.S. citizen may opt out of having a photo taken and request an alternative procedure. CBP works with carriers, airports, and other port facilities to incorporate appropriate notices and processes into their current business models. Examples of such notices are available on CBP's Biometrics Resources website, <https://www.cbp.gov/travel/biometrics/resources>. CBP is aware that, in some cases, adequate signage and notice may not have been installed or provided. CBP seeks to ensure that all locations place signs and notice regarding biometric collection where appropriate.³⁰

²⁷ See DHS/CBP/PIA-056, Privacy Impact Assessment for the Traveler Verification Service (Nov. 14, 2018, as amended) (TVS PIA), available at <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf> (last visited May 15, 2025).

²⁸ See *CBP Privacy Evaluation (CPE) of the Traveler Verification Service (TVS) in support of the CBP Biometric Entry-Exit Program* (Aug. 15, 2022), (CPE TVS Report), available at <https://www.cbp.gov/document/foia-record/cpe-traveler-verification-service-final-report> (last visited May 15, 2025); see also TVS PIA at 1.

²⁹ See CPE TVS Report at 6.

³⁰ See CPE TVS Report at 6.

Upon request, CBP officers provide individuals with a handout (i.e., “tear sheet”) with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular collection method, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.³¹ CBP is aware that some locations may not have had adequate information informing travelers of the availability of a tear sheet for more information. CBP is working to make sure all locations collecting biometrics provide this information and have available tear sheets for travelers. Additionally, in the Federal Inspection Service area (FIS area), CBP posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States.³² Privacy information on the program, such as applicable System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs), are published on the DHS Privacy website, <https://www.dhs.gov/privacy>. CBP will also continue to make program information, such as FAQs, available for the public on CBP’s biometrics website at <https://www.cbp.gov/travel/biometrics>.

7. No Match Procedures

CBP has designed the entry and exit inspection process such that, in the event of a mismatch, false match, or no match, CBP or the carrier may use alternative means to verify the traveler’s identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler’s document should be performed. On entry, the CBP officer may continue to conduct additional screening or request fingerprints (if appropriate) to verify identity. Each inspection booth at entry is equipped with a fingerprint reader. At departure, after the manual review of the travel

³¹ See CPE TVS Report at 6.

³² See CPE TVS Report at 6-7.

document (i.e., scanning a boarding pass and checking a traveler's passport), the airline or cruise line may notify CBP's outbound enforcement teams should additional inspection be required.³³ If the CBP inspection yields no derogatory information, the CBP officer allows the traveler to board/continue travel. If CBP finds actionable derogatory information on the traveler during the additional inspection, the CBP officer may escort the traveler to the FIS area to conduct further questioning and take the appropriate actions under CBP's law enforcement authorities. CBP is aware that in some cases, travelers have been improperly delayed or experienced other adverse consequences due to a mismatch. In the event that an individual does experience a delay or issue as an outcome of these processes, travelers may contact the CBP Information Center and/or DHS Traveler Redress Inquiry Program (TRIP).³⁴ Signage and tear sheets at select ports of entry where the TVS is employed provide information on how to contact the CBP Information Center and/or DHS TRIP. In addition, travelers may request information from the on-site CBP officer or gate agent.

8. U.S. Nationals, Dual Nationals and Lawful Permanent Residents

Under the INA, a U.S. national is either a citizen of the United States, or a person who, though not a U.S. citizen, owes permanent allegiance to the United States. *See* INA 101(a)(22) (8 U.S.C 1101(a)(22)). Alien U.S. national status applies only to individuals who were born either in American Samoa or on Swains Island to parents who are not

³³ Communication between CBP's outbound enforcement team and airlines/cruise lines is not unique to locations where facial comparison is implemented. During the outbound inspection, CBP may interview the traveler as well as use Biometric Exit-Mobile (BE-Mobile) devices. CBP conducts outbound enforcement operations using BE-Mobile devices in all modes of transportation and also at locations where facial comparison technology (i.e., biometric exit boarding) is unavailable. Neither the operations nor the technology is exclusive to locations where facial comparison-based biometric exit is implemented.

³⁴ *See* CBP, CBP Information Center, https://help.cbp.gov/s/?language=en_US (last visited May 15, 2025); DHS, DHS Traveler Redress Inquiry Program (DHS TRIP), <https://www.dhs.gov/dhs-trip> (last visited May 15, 2025).

citizens of the United States.³⁵ Dual nationals are individuals who owe allegiance to both the United States and a foreign country. They are required to obey the laws of both countries, and either country has the right to enforce its laws. For purposes of international travel, U.S. nationals, including dual nationals, must use a U.S. passport (or alternative documentation as required by 22 CFR part 53) to enter and leave the United States. *See* INA 215(b) (8 U.S.C. 1185(b)); 22 CFR 53.1. In cases where dual nationals fail to present the proper travel documents, biometrics may be used to identify that the same individual has traveled using documents issued by different countries.

For purposes of this rule, a U.S. national or dual national who presents as a citizen of another country will be processed as a foreign national and the individual's photo will be retained accordingly, unless the individual is able to present evidence of U.S. citizenship or nationality.³⁶ Under immigration law, lawful permanent residents (LPRs) are aliens authorized to live permanently within the United States.³⁷ As such, for purposes of this rule, LPRs will be processed as aliens.

9. Business Requirements for Public-Private Partnerships

The business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP's facial comparison technology. The Business Requirements Documents are available on CBP's biometrics website at <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy> and are also discussed in the TVS PIA.³⁸ The CBP Business Requirements prohibit CBP's approved

³⁵ *See* U.S. Department of State, Dual Nationality, <https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/Relinquishing-US-Nationality/Dual-Nationality.html> (last visited May 15, 2025).

³⁶ A person claiming U.S. citizenship or nationality must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation as required by 22 CFR part 53. If such person fails to satisfy the examining immigration officer that the traveler is a U.S. citizen, the person shall thereafter be inspected as an alien applicant for admission. 8 CFR 235.1(b).

³⁷ Under section 101(a) of the INA (8 U.S.C. 1101(a)), the term "alien" means any person who is not a citizen or national of the United States. *See also* 8 CFR 215.1(a). Therefore, a lawful permanent resident is an alien under the INA.

³⁸ TVS PIA at 10, 17-18, 21-22.

partners such as airlines, airport authorities, or cruise lines and participating organizations (e.g., vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.³⁹ The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement. To use TVS, private sector partners must agree to these Business Requirements.⁴⁰

IV. Summary of Changes to the Biometric Entry and Exit Regulations

To advance the legal framework for the full implementation of a biometric exit capability as described above, DHS is amending the regulations in parts 215 and 235 of title 8 of the Code of Federal Regulations (8 CFR parts 215 and 235) that set forth the requirements for providing biometrics upon entry and departure as described below.

A. General Biometric Exit Requirement for Aliens

Prior to the effective date of this final rule, the regulations at 8 CFR 215.8(a)(1) authorize DHS to collect biometric exit information from certain aliens on departure from the United States pursuant to pilot programs at air, land, or sea ports of entry and places a limit of 15 air or sea ports of entry at which such biometric exit pilots may be established. The reference to pilot programs and the 15 air or sea port limitation hinder DHS's ability to expand and fully implement a comprehensive biometric exit solution. Therefore, DHS is amending 8 CFR 215.8 by removing the reference to pilot programs and the reference

³⁹ CBP, Biometric Air Exit Business Requirements, v3.0 at 10 (2023), <https://www.cbp.gov/sites/default/files/assets/documents/2023-Oct/Biometric%20Air%20Exit%20Business%20Requirements5.pdf> (CBP Biometric Air Exit Business Requirements); and CBP, Biometric Sea Entry-Exit Business Requirements, v2.0 at 10 (2023), https://www.cbp.gov/sites/default/files/assets/documents/2023-Oct/Sea%20Business%20Requirements%20Document10_0.pdf (CBP Biometric Sea Entry-Exit Business Requirements).

⁴⁰ CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

to 15 air or sea port limit, allowing DHS to establish a general biometric exit requirement for aliens.

B. Collection of Photographs from Aliens Upon Entry and Departure

To implement a biometric entry-exit system based on facial comparison, DHS is amending the regulations to provide that all aliens may be required to be photographed upon departure from the United States. Specifically, DHS is amending 8 CFR 215.8 to add a new paragraph (a)(1), which provides that an alien may be required to be photographed when departing the United States to determine identity or for other lawful purposes. The collection of photographs from an alien upon departure will assist DHS in determining the alien's identity and whether immigration status in the United States has been properly maintained. The exemptions of certain aliens from the collection of biometrics provided in 8 CFR 215.8(a)(1) and (2), redesignated as 8 CFR 215.8(a)(2) and (3) and revised by this final rule, will no longer pertain to the collection of photographs from aliens upon departure and will only apply to the collection of other biometrics.

In addition, DHS is amending 8 CFR 235.1(f) to add new paragraph (f)(1)(ii), which provides that an alien seeking admission may be required to be photographed to determine the alien's identity, admissibility, and whether immigration status in the United States has been properly maintained. Like the collection of photographs upon departure, the exemptions provided in 8 CFR 235.1(f)(1)(ii), redesignated as 8 CFR 235.1(f)(1)(iii) and revised by this final rule, will no longer pertain to the collection of photographs from aliens seeking admission and will only apply to the collection of other biometrics.

As noted above, DHS is retaining the exemptions in 8 CFR 215.8 and 235.1(f)⁴¹ for the collection of biometrics other than photographs (e.g., fingerprints and other biometrics) from aliens upon entry to and departure from the United States. This is set forth in redesignated 8 CFR 215.8(a)(2) and (3) and 235.1(f)(1)(iii) and (vi) as amended by this final rule. Notwithstanding these exemptions, DHS is authorized to collect biometrics from aliens, regardless of age, citizenship, or visa status, for law enforcement purposes or in other contexts not addressed by these regulations, such as from aliens attempting to enter the United States illegally between U.S. ports of entry.

C. Collection of Biometrics When Departing the United States and Other Minor Conforming and Editorial Changes

DHS is amending 8 CFR 215.8(a) to expand where the collection of biometrics may be required. Prior to the effective date of this final rule, 8 CFR 215.8(a)(1) provided that biometrics may be collected from aliens only when departing “the United States from a designated port of entry.” As described above, this final rule adds new paragraph 8 CFR 215.8(a)(1) and redesignates 8 CFR 215.8(a)(1) as 8 CFR 215.8(a)(2). Both new paragraph 8 CFR 215.8(a)(1) and redesignated paragraph 8 CFR 215.8(a)(2) now provide that biometrics may be collected from aliens “when departing the United States” from any location. This amendment is necessary to allow for the collection of biometrics from

⁴¹ The following categories of aliens will remain exempt from the requirements under 8 CFR 215.8 and 235.1 to provide other (non-photograph) biometrics upon arrival to, and departure from, the United States at a U.S. port of entry: Canadian citizens under section 101(a)(15)(B) of the INA who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the date of admission; aliens admitted on A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to these requirements; classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply. See 8 CFR 215.8(a)(1) and (2); and 8 CFR 235.1(f)(1)(ii) and (iv).

individuals upon departure at locations other than from a designated port of entry.⁴²

Although the majority of travelers depart the United States from a designated port of entry, a few travelers depart the country from locations that are not designated as ports of entry, including airports such as Ronald Reagan Washington National Airport⁴³ as well as other locations such as pleasure boat docks that are not designated ports of entry. To ensure the implementation of a biometric entry-exit system that tracks all individuals departing the United States, DHS may require aliens to provide biometrics upon departure from designated ports of entry or from any other location.

In addition, DHS is making certain minor conforming and editorial changes in 8 CFR 215.8 and 235.1(f). In 8 CFR 215.8, DHS is redesignating paragraphs (a)(1) and (2) as paragraphs (a)(2) and (3), and revising cross-references and adding paragraph headings as necessary. In § 235.1(f), DHS is redesignating paragraphs (f)(1)(ii), (iii), and (iv) as paragraphs (f)(1)(iii), (v), and (vi), respectively; adding new paragraphs (f)(1)(ii) and (iv); and revising cross-references and adding paragraph headings as necessary. In both §§ 215.8 and 235.1(f), DHS is removing the phrase “[t]he Secretary of Homeland Security or his or her designee” and adding in its place “DHS”, and removing the phrase “biometric identifiers” and adding in its place “biometrics.”

Finally, DHS is amending 8 CFR 215.8(a) and 235.1(f) to remove the specific references to fingerprints and photographs. Prior to the effective date of this final rule, 8 CFR 215.8(a)(1) and 235.1(f)(1)(ii) provided that any alien may be required “to provide fingerprints, photograph(s) or other specified biometric identifiers” upon arrival into or departure from the United States. Because this final rule adds new paragraphs relating to

⁴² Designated ports of entry are listed in 8 CFR 100.4(a) for aliens arriving by vessel or by land transportation and in 8 CFR 100.4(b) for aliens arriving by aircraft.

⁴³ This airport is not a port of entry pursuant to 8 CFR 100.4(b) and does not have federal inspection processes or facilities, but it still has a few flights that depart to international locations, mostly those that have CBP preclearance facilities (typically in Canada or the Caribbean).

the provision of photographs, the word “photograph(s)” in these provisions is no longer appropriate. Furthermore, to allow the flexibility for DHS to employ different methods of biometric collection in the future as biometric technology advances, DHS is amending 8 CFR 215.8(a) and 235.1(f) to provide instead that any alien, other than those exempt by regulation, may be required “to provide other biometrics” upon arrival into and departure from the United States. *See* 8 CFR 215.8(a)(2) and 235.1(f)(1)(iii). For example, CBP has tested iris technology, and there may be other biometric options that may have potential for implementation in the future.

V. Discussion of Comments Submitted in Response to the NPRM

A. Overview

In response to the NPRM, DHS received 320 comments during the two 30 day public comment periods. Commenters consisted of individuals, advocacy groups, legal service providers, professional associations, State and local governments, and social organizations. The comments and responses are grouped by subject area. Some commenters expressed support for the rule and/or offered suggestions for improvement. The majority of commenters expressed general opposition to the rule, mentioning immigration policy concerns, general privacy concerns, and economic concerns.

B. Discussion of Comments

1. Comments Expressing General Support

Comment: Several commenters generally supported the proposed rule, providing various rationales or supporting data. Commenters noted that biometrics will streamline the travel process, address national security concerns, provide U.S. citizens with the opportunity to request alternative screening procedures and protect children from being exploited by human traffickers.

Response: DHS appreciates the support for the rule and agrees that the rule will streamline the travel process and address various national security concerns to include

terrorism and nonimmigrants who overstay their authorized period of admission.

Furthermore, DHS agrees that the rule preserves the ability for U.S. citizens to request alternative procedures for identity verification. DHS also agrees that this rule will protect youth and children from being exploited by human traffickers; please see the response in Section V.B.4.1., *Under 14 Children: Privacy, Authority and Accuracy Concerns*, below for additional details regarding the benefits of collecting biometrics from children under the age of 14.

2. Comments Expressing General Support with Recommendations

Comment: Some commenters expressed support for the rule and offered suggestions for improvement. Commenters supported CBP's efforts to maintain the ability for U.S. citizens to request alternative screening procedures and applauded CBP's efforts to institute privacy protections for all travelers. Commenters noted that an expanded system-wide biometric implementation will not only facilitate travel to include a more hygienic user experience, but also address national security concerns arising from fraudulent documents and those individuals that overstay their authorized period of admission. Several commenters supported DHS's decision to withdraw the 2008 NPRM⁴⁴ which proposed to require commercial air and vessel carriers to collect biometric information from certain aliens departing the United States and submit this information to DHS within a certain timeframe.

Response: DHS appreciates the support for the rule that provides for continued implementation of the statutorily mandated biometric entry-exit system. DHS also appreciates support for the withdrawal of the 2008 NPRM. DHS agrees that this final rule will streamline the travel process and address various national security concerns to

⁴⁴ 73 FR 22065 (Apr. 24, 2008).

include fraudulent documents and aliens who overstay their authorized period of admission. Furthermore, DHS agrees that the rule preserves the ability for U.S. citizens to request alternative procedures.

a. Recommendation: Provide additional information for both the traveling public and stakeholders regarding U.S. citizens' voluntary participation in the program.

Comment: Commenters suggested that to instill greater public confidence in the program, CBP should further clarify the option for U.S. citizens to opt out of the program and establish a rule dictating that U.S. citizens' photos may only be kept for up to 12 hours.

Response: DHS agrees that U.S. citizens should have proper notification of their option to opt-out of facial comparison. This issue is further discussed in Section V.B.4.e., *U.S. Citizen Opt-Out*, below, including a discussion regarding CBP's authorities, signage/notification, alternative procedures, and training efforts. CBP agrees that the appropriate retention period for U.S. citizen photos should be no more than 12 hours. The National Archives and Records Administration (NARA)-approved records schedule requires destruction of U.S. citizen photos upon confirmation of U.S. citizenship and no later than 12 hours after confirmation of U.S. citizenship. CBP worked closely with the NARA to approve the retention period for U.S. citizen photos.⁴⁵

Comment: One commenter suggested that both U.S. citizens and aliens should be required to have their photo taken upon arrival/departure.

Response: CBP initially considered including U.S. citizens in its biometric entry-exit program because having separate processes for aliens and U.S. citizens at ports of

⁴⁵ See DHS, CBP, U.S. Citizen Encounter Photos (DAA-0568-2019-0002), available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/departments-of-homeland-security/rg-0568/daa-0568-2019-0002_sfl15.pdf (last visited May 15, 2025).

entry creates logistical and operational challenges that affect security, wait times, and the traveler experience. However, CBP determined that the best course of action at this time is to continue to allow U.S. citizens to voluntarily participate in the biometric entry-exit program. CBP does not have plans at this time to require U.S. citizens to be photographed when entering or exiting the United States, as evidenced by DHS's withdrawal of the 2008 NPRM proposing to require biometric collection from U.S. citizens. *See* Withdrawal Notice (85 FR 73644).

Nevertheless, to carry out its responsibilities effectively under the INA, for both arrivals and departures from the United States, CBP must be able to determine conclusively whether a traveler is a U.S. citizen or national or an alien by verifying that the traveler is the true bearer of the presented travel documentation. CBP is authorized to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter material or relevant to the enforcement or administration of the INA. *See* INA 287(b) (8 U.S.C. 1357(b)). A person claiming U.S. citizenship must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation. *See* INA 215(b) (8 U.S.C. 1185(b)), 8 CFR 235.1(b), and 22 CFR 53.1.

b. Recommendation: Increase program transparency to address concerns from privacy advocates and members of Congress.

Comment: Commenters suggested that CBP should provide the public with additional information about the biometric entry-exit program such as data usage, retention, protection, and dissemination, as well as continually update Privacy Impact Assessments and SORNs as biometric technology capabilities and methodologies continue to evolve.

Response: CBP endeavors to provide notice to the public continuously regarding the biometric entry-exit program including through regular updates of its PIAs and

SORNs as well as the CBP biometric website at <https://www.cbp.gov/travel/biometrics>. See Section V.B.4.d., *Public Notification and Information*, below, for more information on CBP's transparency and communication efforts. See Section V.B.3.c., *Data Security, Retention, and Dissemination Concerns*, below, for more information regarding CBP's data usage, storage, and protection. Additional information is also available in various places on the CBP and DHS websites including <https://www.cbp.gov/travel/biometrics> and <https://www.dhs.gov/privacy>, which provide the relevant PIA and SORN, and which are all updated regularly as capabilities and technologies evolve; and <https://www.dhs.gov/compliance>, which includes information on compliance including periodic reviews of Privacy Threshold Analyses (PTAs), PIAs, and SORNs.

Comment: One commenter suggested that CBP work to make sure travelers understand and adjust to the new system in advance of making biometric collection fully mandatory.

Response: As mentioned in the NPRM⁴⁶, through the CBP biometrics website at <https://www.cbp.gov/travel/biometrics>, and the TVS PIA,⁴⁷ CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII. CBP has also gradually rolled out the biometric entry-exit program with various voluntary pilots over the past several years giving the public the opportunity to adjust to this new process. As discussed throughout this final rule, CBP is still in the process of determining the best way to fully implement biometric collection at all entry and exit modalities. CBP has maintained a proactive approach to stakeholder engagement and outreach through participation in speaking engagements, conferences, and stakeholder meetings. This outreach has kept CBP on the forefront of domestic and

⁴⁶ See the NPRM, 85 FR at 74177 for more information on CBP's protection of PII.

⁴⁷ See TVS PIA at 19.

international engagement by allowing CBP the opportunity to partner with airlines, airport authorities, travel associations and agents, embassies, attachés, and privacy advocacy groups to share programmatic updates on CBP's use of biometric facial comparison technology in the air, land, and sea environments.

CBP also participates regularly in events sponsored by travel industry partners to provide updates which highlight the benefits of biometric facial comparison technology. Some of these partners have included but are not limited to the U.S. Travel Association (USTA), Global Business Travel Association (GBTA), Cruise Line Industry Association (CLIA), American Association of Airport Executives (AAAE), and Airlines for America (A4A), to name just a few. Moreover, to maximize messaging efforts, CBP has often participated in these events in collaboration with its government partners, like TSA or the Science and Technology Directorate (S&T) of DHS.

Comment: Commenters also suggested that CBP set a minimum acceptable accuracy rate consistent across demographics, which, along with system improvements, should then be studied and publicized regularly. One commenter encouraged CBP to expedite the implementation of the 2020 U.S. Government Accountability Office (GAO) audit.⁴⁸

Response: CBP appreciates the commenters' suggestions regarding tracking accuracy rates and effectiveness of improvements to the matching algorithm. CBP does have a minimum acceptable accuracy rate for the program and does regularly track it to ensure program success. CBP's Biometric Air Exit Key Performance Parameters (KPPs) mandate that the system's True Acceptance Rate (TAR) must equal or exceed 97 percent of all in-scope travelers (as previously defined by 8 CFR 215.8 and 235.1) and that the

⁴⁸ See GAO, GAO-20-568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (2020), available at <https://www.gao.gov/products/gao-20-568> (last visited May 15, 2025).

system's False Acceptance Rate (FAR) must not exceed 0.1 percent of all in-scope travelers. Through congressionally mandated reports, such as the annual DHS Entry/Exit Overstay Report⁴⁹ the TSA and CBP: Deployment of Biometric Technologies Report to Congress,⁵⁰ and other public reports, such as the annual CBP Trade and Travel Report,⁵¹ CBP discusses the accuracy rates of the Biometric Entry-Exit program as well as system improvements. Additionally, CBP continues to collaborate with DHS S&T, DHS Office of Biometric Identity Management (OBIM), and the National Institute of Standards and Technology (NIST) on technical standards and evaluation to ensure optimal system performance.

CBP concurred with the 2020 GAO audit recommendations and has addressed each recommendation, as indicated in the Recommendations for Executive Action Table on the applicable GAO website.⁵²

c. Recommendation: Provide additional information regarding no match and opt-out procedures.

Comment: Several commenters requested that CBP clarify its process for when a traveler screening yields a no-match result, to include when CBP assistance should be requested. One commenter also requested the number of Biometric Exit-Mobile devices CBP currently has in use today, as they will likely be used for both no-match and opt-out procedures. Additionally, one commenter indicated that CBP should be responsible for the implications of a no-match result.

⁴⁹ This report is available for FY22 at https://www.dhs.gov/sites/default/files/2023-07/23_0707_FY22_FY23_CBP_Integrated_Entry_Exit_Overstay_Report.pdf and available for previous FYs at <https://www.dhs.gov/publication/entryexit-overstay-report> (last visited May 15, 2025).

⁵⁰ This 2019 DHS report is posted in the docket for this rulemaking.

⁵¹ This report is available for FY22 and earlier at <https://www.cbp.gov/document/annual-report/cbp-trade-and-travel-fiscal-year-2022-report> (last visited May 16, 2025).

⁵² See GAO, GAO-20-568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, Recommendations, Recommendations for Executive Action Table, <https://www.gao.gov/products/gao-20-568> (last visited May 15, 2025).

Response: As discussed in the NPRM, in the event of no match at departure, the carrier or CBP officer will perform a manual review of the travel document (i.e., scanning a boarding pass and checking a traveler's passport).⁵³ If additional inspection is required by a carrier, the carrier line may notify CBP's outbound enforcement teams, but the carrier is not required to do so. Carrier partners should follow internal business rules and policy to manually verify identity and determine boarding status of a traveler. Air carrier and airport partners may contact CBP, in accordance with existing guidelines outlined by the Carrier Liaison Program, when there are issues or concerns with U.S. entry requirements, human trafficking, traveler assessment, fraudulent document detection and imposter identification.⁵⁴

CBP may use mobile devices with the relevant CBP-built mobile applications to support its multilayered enforcement approach. These CBP applications include the Biometric Exit Mobile application. Additional information about the Biometric Exit Mobile application can be found in the Biometric Exit Mobile Program PIA.⁵⁵ CBP officers can use the application on any CBP smartphone. CBP does not dedicate phones to a single mobile application or operation. Rather, officers use these phones to perform various job responsibilities across multiple environments. Ports are provided with enough phones to meet their mobile mission including biometric exit operations. The port will make a determination on how officers will use their phones on a day-by-day basis based on staffing and other law enforcement-related factors.

Comment: One commenter expressed concern that CBP will not have the staffing resources to conduct outbound enforcement operations efficiently.

⁵³ See the NPRM, 85 FR at 74177, for further discussion of no match procedures.

⁵⁴ CBP, Carrier Information Guide: United States Document Requirements for Travel (2023), available at <https://www.cbp.gov/sites/default/files/assets/documents/2023-Nov/Carrier%20Information%20Guide%20ENGLISH.pdf> (last visited May 15, 2025).

⁵⁵ The updated 2018 PIA for DHS/CBP/PIA-026 Biometric Exit Mobile Program, and all prior versions, are available at <https://www.dhs.gov/publication/biometric-exit-mobile-air-test> (last visited May 15, 2025).

Response: CBP has partnered with multiple stakeholders, including airports and airlines, who are assisting with facilitating the collection at departure through the use of CBP's TVS. TVS provides an automated mechanism to verify the identities of travelers. CBP has also partnered with cruise operators in the entry environment and CBP expects these partnerships will also aid in developing a strategy for biometric exit in the sea environment as well. CBP is still determining the best method for using facial biometrics at land exit.

Comment: One commenter requested further clarification on the process for families traveling with children, and persons with reduced mobility as experience during the trials has shown that collecting biometric information from these travelers can be difficult and time consuming.

Response: Air carriers may use discretion when processing travelers with disabilities and families with children, including conducting manual identity verification using the individual's travel document (document review), as is performed for all flights where biometric processing is not available. Additionally, carriers must abide by existing local, state, and federal laws and regulations regarding processing persons with disabilities.

CBP's biometric entry-exit program does not contradict existing accessibility regulations and processes. In many cases, biometric collection equipment accommodates disabilities; furthermore, it is CBP's policy to afford persons with disabilities an equal opportunity to participate in, or benefit from, CBP-conducted services, programs, and activities and to provide reasonable modifications to its services, programs, and activities to qualified individuals with a disability when necessary to avoid discrimination on the basis of disability.

d. Recommendation: Clarify the impact that a biometric exit system would have on airport operations and infrastructure requirements for airports and airlines.

Comment: Commenters requested that CBP explain whether the program's implementation would require separate screening lines, separate processes, or notifications for passengers. Additionally, one commenter requested clarification on whether non-U.S. citizens could opt out of the biometric exit process to avoid additional burdens on CBP and/or the carriers during boarding such as separate boarding queues (i.e., one for U.S. citizens and one for aliens).

Response: As noted throughout this rule, on the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, sex, race and nationality. As indicated on privacy signage, also available on CBP's biometrics website, <https://www.cbp.gov/travel/biometrics/resources>, if a traveler is a U.S. citizen and does not wish to have a photograph taken, the traveler may see a gate agent or CBP officer to request alternative procedures for identity verification. The alternative procedures are intended to be similar to the existing processes at entry and exit. See Section V.B.4.e., *U.S. Citizen Opt-Out*, below, for more information regarding CBP's authorities, signage/notification, alternative procedures, and training efforts. CBP will continue its transparency and communication efforts, discussed in detail in Section V.B.4.d., *Public Notification and Information*, below, as it rolls out full implementation of the biometric entry-exit program.

e. Recommendation: Provide details should airlines/airports choose not to participate in the Biometric Entry-Exit Program.

Comment: Several commenters requested that CBP provide procedures that airlines should follow if they decide not to participate in this voluntary program and that

CBP should commit to continue working with those airports that do not participate in the program.

Response: Participation in CBP's biometric entry-exit program will remain voluntary for carriers under this final rule. If air carriers or airports do not participate, they will continue conducting manual identity verification. However, CBP may supplement this verification with CBP officers conducting periodic biometric exit operations. CBP uses its Workload Staffing Model to determine the staffing requirements and help make allocation decisions for CBP officers at ports of entry, including airports. CBP will continue to use this data-driven methodology to identify staffing requirements by considering all the activities performed by CBP officers at ports of entry, the volume of those activities, and the levels of effort required to carry them out.

f. Recommendation: Provide carrier protections through the SAFETY Act.

Comment: Some commenters recommended that DHS provide SAFETY Act⁵⁶ legal liability protections for air carriers that participate as partners in CBP's biometric entry-exit program. The commenters stressed the importance of these protections against claims of discrimination in facial comparison technology, as well against any breach of traveler privacy.

Response: DHS will not issue a blanket liability protection. Carriers need to work with their technology providers on seeking SAFETY Act certification for biometric technology devices. The SAFETY Act also is designed for anti-terrorism technology certification, not for general privacy or other areas of discrimination concerns. The SAFETY Act offers liability protection to sellers of qualified anti-terrorism technologies

⁵⁶ Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, Pub. L. 107-296, 116 Stat. 2135, 2238 (6 U.S.C. 441 *et seq.*).

to incentivize the development and deployment of anti-terrorism technology solutions.

Additional information is available on the DHS S&T SAFETY Act website at

<https://www.safetyact.gov/>.

g. Recommendation: Establish an oversight body on DHS biometric programs.

Comment: One commenter supports the findings and recommendations in the Homeland Security Advisory Council Biometrics Subcommittee 2020 Report,⁵⁷ including the establishment of a DHS Biometrics Oversight and Coordination Council.

Response: While DHS has not created the specific oversight council as suggested in the 2020 report, numerous oversight processes exist to ensure DHS compliance with civil rights and civil liberties. These processes included congressional hearings, congressionally mandated status update reports and responses to formal congressional inquiries. See Section V.B.4.j., *Government Accountability and Oversight*, below for more information on the various biometric oversight and accountability mechanisms.

h. Recommendation: Provide more information on the implications of state/local laws and implementation of biometric capabilities in the land and sea environments.

Comment: One commenter requested that CBP provide additional guidance and clarification on the role of the biometric entry-exit program when local laws conflict with CBP's biometric entry-exit strategy. One commenter indicated that further details on process, timing, cost, etc., in the land and sea environments are necessary to ensure traveler confidence and comprehension.

⁵⁷ Homeland Security Advisory Council, Final Report of the Biometrics Subcommittee (2020) (HSAC Biometrics Report), available at https://www.dhs.gov/sites/default/files/publications/final_hsic_biometrics_subcommittee_report_11-12-2020.pdf (last visited May 15, 2025).

Response: CBP is congressionally mandated to implement a Biometric Entry-Exit System and is issuing this regulation to implement such system. The Supremacy Clause of the U.S. Constitution provides that federal laws and treaties are the supreme laws of the land, and it is well established that the power to regulate immigration is exclusively with the federal government. In instances where a state law conflicts with federal immigration laws, the state law must yield. See Section V.4.B.s, *Land and Sea Implementation*, below, for more information on CBP’s implementation plan in the land and sea environments.

i. Recommendation: Further coordinate with NIST to examine existing standards that may unintentionally inhibit CBP’s ability to consider other biometric modalities.

Comment: One commenter requested that CBP coordinate with NIST to ascertain gaps that could limit consideration of other biometric modalities – e.g., edge computing platforms, mobile platforms, and cloud-based systems.

Response: CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance regarding facial comparison capabilities as well as remaining informed on the development and evolution of other biometric modalities, especially as it relates to the border security mission.⁵⁸

j. Recommendation: Implement additional changes to the rule to ensure all aliens arriving to and departing from the United States are thoroughly screened and vetted.

Comment: One commenter requested that CBP remove all age restrictions in 8 CFR 215.8 and 235.1 for all biometric collection regardless of biometric modality and

⁵⁸ See, e.g., DHS/OBIM/PIA-005 Office of Biometric Identity Management (OBIM)-National Institute of Standards of Technology (NIST) Data Transfer 3-5 (2022), available at <https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards> (last visited May 15, 2025).

expand biometric collection to include additional biometric modalities (e.g., iris, DNA, voice). Additionally, the commenter requested that DHS finalize both the USCIS and CBP biometrics rules.

Response: The NPRM published on September 11, 2020, entitled “Collection and Use of Biometrics by U.S. Citizenship and Immigration Services,” 85 FR 56338 (USCIS NPRM), would have implemented the suggested changes if finalized.⁵⁹ On May 10, 2021, DHS withdrew the USCIS NPRM. 86 FR 24750. However, since the withdrawal of the NPRM, the President has issued Executive Order No. 14161, *Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats*, 90 FR 8451, (Jan. 30, 2025) (E.O. 14161). E.O. 14161 mandates that DHS protect the American public from “aliens who intend to commit terrorist attacks, threaten our national security, espouse hateful ideology, or otherwise exploit the immigration laws for malevolent purposes” and to “vet and screen to the maximum degree possible all aliens who intend to be admitted, enter, or are already inside the United States.” Therefore, DHS will consider future efforts to enhance biometric submission to further the goals of this Executive Order.

Through this rulemaking, DHS is removing the age restrictions for photograph collection under 8 CFR 235.1 for aliens seeking admission to the United States, as well as under 8 CFR 215.8 for aliens departing the United States. See Section V.B.4.1, *Under 14 Children: Privacy, Authorities and Accuracy Concerns*, below, for more details.

3. Comments Expressing General Inquiries

a. Rule Impact

Comment: Commenters raised questions regarding to whom the rule applies, as well as the purpose and need for the biometric information collected.

⁵⁹

Response: As stated throughout this rule, on the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, sex, race and nationality. DHS is mandated by numerous statutes as discussed above⁶⁰ to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient.

This final rule improves DHS's ability to meaningfully implement a comprehensive biometric entry-exit system and make the process for verifying the identity of aliens more efficient, accurate, and secure by using facial comparison technology. Implementing an integrated biometric entry-exit system that verifies the identity of aliens at arrival and on exit and then uses that information to confirm that the alien has exited as required is essential for addressing the national security concerns arising from the threat of terrorism, combatting the fraudulent use of legitimate travel documentation, and identifying aliens who overstay their authorized period of admission or are present in the United States without being admitted or paroled. An integrated biometric entry-exit system can also fill the gaps left by incorrect or incomplete biographic data for travelers.

b. Technology Usage and Techniques Accuracy and Misidentification

Comment: Several commenters raised questions on the training dataset and machine learning models used for facial comparison.

⁶⁰ Two of the relevant statutes are section 110 of the DMIA (8 U.S.C. 1365a) and section 7208 of the IRTPA (8 U.S.C. 1365b). For a more complete list, please refer to Section II.B. of this final rule.

Response: The information requested regarding the training dataset and machine learning models CBP uses for facial comparison is proprietary information. CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance regarding facial comparison capabilities. NIST has conducted in-depth analysis on facial comparison algorithms, which showed that the vendor selected by CBP is capable of delivering algorithms with a high accuracy rate.⁶¹ For more information on NIST's analysis, see Section V.B.4.k, *Accuracy, General Bias, and Misidentification Concerns*, below.

CBP has issued PIAs for many pilots that were testing/developing facial comparison technology. These PIAs include information about how the algorithms are tested to assure accuracy of the facial comparison technology.⁶²

For more information on how CBP ensures high accuracy rates across all demographics see Section V.B.4.k., *Accuracy, General Bias, and Misidentification Concerns*, below.

c. Data Security, Retention, and Dissemination Concerns

Comment: Many commenters had questions regarding the safety and protection of sensitive information with use of this technology and linkage to interagency databases. Additionally, one commenter asked whether protection would be provided to the individuals should a breach or cybersecurity incident occur. One commenter asked if CBP could delete the biometric information but retain the record of the entry or exit.

⁶¹ See NIST, NISTIR 8280, FRVT Part 3: Demographic Effects 8, 26 (2019) (NIST FRVT Demographic Effects Report), available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf> (last visited May 15, 2025).

⁶² See, e.g., DHS/CBP/PIA-025 1:1 Facial Comparison Project, DHS/CBP/PIA-026 Biometric Exit Mobile Air Test, DHS/CBP/PIA-027 Southwest Border Pedestrian Exit Field Test, DHS/CBP/PIA-030 Departure Information Systems Test, and the TVS PIA. These PIAs are available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection> (last visited May 16, 2025).

Response: Because numerous federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data to verify their identities, and authenticates travel documents, DHS cannot delete personally identifiable data and only retain a record of entry-exit. Furthermore, DHS retains certain records for up to 75 years, which is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.⁶³

When DHS personnel discover a suspected or confirmed privacy incident, there are a series of actions and activities that must occur to appropriately report, investigate, respond, and mitigate the privacy incident. DHS's policy for responding to privacy incidents is established in the DHS Privacy Office, DHS Instruction Guide 047-01-008, Privacy Incident Handling Guidance (2017).⁶⁴ Additionally, DHS Privacy Policy Instruction 047-01-006, Privacy Incident Responsibilities and Breach Response Team (2017),⁶⁵ provides additional instruction on how DHS and CBP employees should handle and respond to privacy incidents. The Breach Response Team determines the appropriate course of action with respect to any privacy incident investigation, remedy options,

⁶³ See DHS/NPPD/PIA-002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) 25 (2012) (IDENT PIA), available at <https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system> (last visited May 16, 2025) (note that this website refers to this PIA as "DHS/OBIM/PIA-001" due to OBIM renumbering after the DHS National Protection and Programs Directorate (NPPD) became the Cybersecurity and Infrastructure Security Agency within DHS); and DHS/OBIM/PIA-004, Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA (2020) (HART PIA), available at <https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1> (last visited May 16, 2025).

⁶⁴ Available at https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf (last visited May 16, 2025).

⁶⁵ Available at <https://www.dhs.gov/sites/default/files/publications/047-01-006%20Privacy%20Incident%20Responsibilities%20and%20Breach%20Response%20Team%20FINAL%2012-04-17.pdf> (last visited May 16, 2025).

resource allocations, risk mitigation, and interagency engagement. DHS and CBP also follow OMB’s breach response guidance, including OMB M-17-12 and M-25-04.⁶⁶

For more information on how CBP safeguards sensitive information, see Section V.B.4.g., *Data Security, Retention, and Dissemination Concerns*, below.

4. Comments Expressing General Opposition

a. *General Opposition*

Comment: Some commenters provided general opposition for the proposed rule, with little, non-specific reasoning or justification provided.

Response: DHS appreciates the time these commenters took to read the rule, but DHS respectfully disagrees. DHS’s intent for this rule is explained in detail in the rule’s preamble and throughout the NPRM. DHS is mandated by numerous statutes to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Additionally, DHS gave careful consideration to the costs and benefits associated with this regulatory change, as well as considered all of the comments submitted by the public. DHS concludes that after the careful weighing of equities, this rulemaking is necessary as biometrics are simply a more efficient and reliable means of identifying an individual, compared to biographic identifiers.

Comment: Some commenters requested that DHS not use the term “alien” in the rule.

⁶⁶ See OMB M-17-12, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf (last visited July 31, 2025) and OMB 25-04, available at <https://www.whitehouse.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf> (last visited July 31, 2025).

Response: DHS used the term “noncitizen” in the NPRM except where quoting directly from statutory or regulatory text that uses the term “alien.” However, DHS uses the term “alien” in this final rule consistent with the statutory and regulatory text.

Comment: Two commenters suggested that DHS should be abolished.

Response: Comments suggesting DHS be abolished are outside the scope of this rulemaking. DHS and its homeland security mission are born from the commitment and resolve of Americans across the United States in the wake of the September 11, 2001, attacks. With the enactment of the Homeland Security Act in November 2002, DHS formally came into being as a stand-alone, Cabinet-level department to further coordinate and unify national homeland security efforts, opening its doors on March 1, 2003. As the complex threat environment continues to evolve, DHS will embody the relentless resilience of the American people and continue to ensure a safe, secure, and prosperous homeland.

Comment: One commenter expressed concern that the use of technology would cause officers to distance them physically from the subject and/or distance them from personal responsibility for tasks done.

Response: CBP’s mission is to protect the American people, safeguard our borders, and enhance the nation’s economic prosperity. Technology will never replace the skills and capabilities that can only be exhibited by CBP’s personnel in identifying and mitigating threats to the nation. In fact, studies⁶⁷ have shown that it is the combination of humans, with technology at their disposal, that best serve the CBP

⁶⁷ See P. Jonathon Phillips, et al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, 115 PNAS 6171 (2018), <https://www.pnas.org/content/pnas/115/24/6171.full.pdf> (last visited May 16, 2025). See also Hamood M. Alenezi & Markus Bindemann, The Effect of Feedback on Face-Matching Accuracy, 27 Applied Cognitive Psych. 735 (2013), <https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.2968> (last visited May 16, 2025); and Matthew C. Fysh & Markus Bindemann, Effects of time pressure and time passage on face-matching accuracy, 4 Royal Soc’y Open Sci. 170249 (2017), <https://royalsocietypublishing.org/doi/full/10.1098/rsos.170249#RSOS170249C16> (last visited May 16, 2025).

mission while simultaneously respecting the rights of all persons. Humans, balanced with technology, are essential to successful execution of these biometric programs.

CBP's investment in technology is designed to empower officers to execute the agency's critical law enforcement mission and alleviate the administrative burden on officers so they are able to focus on enforcement. The use of facial comparison technology saves frontline officers' time in matching travelers to document photos and capturing fingerprints CBP already has in its holdings, allowing for a focus on threat detection and behavioral indicators that technology cannot identify. CBP's workforce is critical to accomplishing CBP's missions.

b. General Privacy Concerns

Comment: Many commenters disagreed with the rule, stating that the proposal is unnecessary, offensive, an invasion of privacy, infringes on freedoms, and would violate the respect, privacy rights, and civil liberties of U.S. citizens, legal immigrants, aliens, victims of domestic violence, other vulnerable parties, and children.

Response: DHS disagrees with these comments. DHS recognizes there may be increased sensitivities associated with facial comparison technology. However, DHS complies with all applicable privacy statutes, regulations, and policies. Further, DHS currently includes information about specific privacy protections in the relevant PIAs. The PIAs also direct individuals to the applicable SORNs, which describe the categories of individuals covered by the system, categories of records in the system, legal authority for maintaining the system, purpose of the system, and routine uses of records maintained in the system. All PIAs and SORNs are submitted to the DHS Privacy Office for review and approval by the DHS Chief Privacy Officer.

The privacy compliance documentation process is an iterative process that not only provides transparency into the details of DHS activities, but also shapes those activities by identifying privacy risks as well as mitigations and privacy-enhancing

solutions. Privacy is a DHS-wide responsibility, and the DHS Privacy Office works with DHS components, including CBP, to ensure privacy protections are incorporated in the entire lifecycle of DHS projects, programs, and activities. DHS is committed to the fair and equal treatment of all individuals in its screening and vetting activities, ensuring the rights of all people are protected, while taking lawful actions necessary to secure the homeland. In addition to adhering to all relevant statutory and regulatory privacy protections, DHS complies with existing DHS policies, which include the DHS Fair Information Practice Principles (FIPPS)⁶⁸ that ensure privacy safeguards are incorporated throughout the information lifecycle. These safeguards also account for administrative, physical, and technical controls to ensure appropriate collection, use, maintenance, and protection of all information, both biometric and biographic, submitted to DHS. Furthermore, DHS complies with protections in 8 U.S.C. § 1367 regarding disclosure of information pertaining to beneficiaries of applications for victim-based immigration relief. DHS will continue to adhere to all statutes, regulations, and policies regarding the privacy rights of individuals departing or entering the United States.

Comment: Some commenters stated the rule violates the fundamental human rights to privacy, provided specifically in Articles 17 and 26 of the International Covenant on Civil and Political Rights (ICCPR)⁶⁹ and Article 12 of the Universal Declaration of Human Rights (UDHR),⁷⁰ which the United States has ratified.

Response: DHS disagrees with commenters that this rule violates any provisions of international law that are applicable within the United States. The tenets of the rights

⁶⁸ DHS, The Fair Information Practice Principles, <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles> (last visited May 16, 2025).

⁶⁹ The text of the ICCPR is available on the United Nations Office of the High Commissioner for Human Rights website, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (last visited May 16, 2025).

⁷⁰ The text of the Universal Declaration of Human Rights is available on the United Nations website, <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (last visited May 16, 2025).

to privacy expressed under the ICCPR and UDHR are already incorporated into U.S. domestic law via the Privacy Act and through DHS regulations and policy guidance. DHS is committed to fair equal treatment of all individuals and the rule complies with all applicable privacy statutes, regulations, and policies.

Comment: Two commenters mentioned the 2020 DHS Office of the Inspector General (OIG) Report on DHS Privacy oversight inefficiencies.

Response: CBP is aware of the DHS OIG report on its November 2020 audit, entitled “DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives”⁷¹ (Nov. 2020 DHS OIG Report). CBP takes privacy very seriously and is dedicated to protecting the privacy of all travelers. DHS OIG identified three recommendations for the DHS Privacy Office to improve privacy compliance, information sharing access agreements, and privacy training.⁷² Two of the recommendations apply to internal record keeping (compliance and training) and the third applies to oversight of information sharing and access agreements.⁷³ None of those recommendations was specific to this rulemaking. CBP reviews all programs and changes to programs to determine any privacy concerns and mitigate any privacy risks.

c. Privacy Act and Paperwork Reduction Act

Comment: Some commenters stated that the proposed rule fails to justify its claimed authority to collect biometrics from U.S. citizens or lawful permanent residents (LPRs) protected by the Privacy Act (5 U.S.C. 552a).

Response: DHS respectfully disagrees with the commenters. In the NPRM, DHS explains in great detail its authority to collect biometrics from all aliens, including

⁷¹ DHS OIG, OIG-21-06, DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives (2020), available at <https://www.oig.dhs.gov/sites/default/files/assets/2020-12/OIG-21-06-Nov20.pdf> (last visited May 16, 2025).

⁷² Nov. 2020 DHS OIG Report at 17.

⁷³ Nov. 2020 DHS OIG Report at 17.

LPRs.⁷⁴ Moreover, DHS is authorized to take and consider evidence concerning the privilege of any person, including U.S. citizens, to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and DHS regulations. *See* INA 287(b) (8 U.S.C. 1357(b)). The Privacy Act does not prevent government agencies from collecting information about U.S. citizens and LPRs when needed for the agency to execute its statutory and regulatory responsibilities, but rather requires that the government follow a process for appropriately protecting information and informing the public about collection and retention of the information. Additionally, as noted here and elsewhere throughout this final rule, U.S. citizens are not required to but can voluntarily participate in the facial biometric process.

DHS acknowledges that the Privacy Act requires that “each agency that maintains a system of records shall...collect information to the *greatest extent practicable* directly from the subject.” 5 U.S.C. 552a(e)(2) (emphasis added), subject to any exemptions from this provision contained in 5 U.S.C. 552(j) and (k). Nevertheless, as explained in the NPRM, CBP considered and piloted many types of biometrics collections.⁷⁵ Using information gleaned from the pilots as well as public feedback, CBP has concluded that partnering with carriers and airports to capture facial images is the most viable large-scale solution as it is highly effective, cost effective, and less disruptive than other possible methods.

Comment: One commenter stated that CBP should require airlines and airports to display the Office of Management and Budget (OMB) control number regarding this information collection.

⁷⁴ *See* the NPRM, 85 FR at 74164, for more information on DHS’ authority to collect biometrics from all aliens.

⁷⁵ *See* the NPRM, 85 FR at 74171, for more information about CBP’s biometrics pilots.

Response: The OMB control number, 1651-0138, is listed in the TVS PIA.

Furthermore, pursuant to the Paperwork Reduction Act of 1995 (“Paperwork Reduction Act”), CBP displays the OMB control number on signage. *See* 44 U.S.C. 3507. CBP also provides language for signs that are printed and displayed by airlines, airports and other carriers at each location where biometric collection takes place. Additionally, for the convenience of the public, CBP updated its biometrics website regarding CBP’s Biometric Privacy Policy, <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>, to include the OMB control number.

d. Public Notification and Information

Comment: Several commenters raised concerns regarding a perceived lack of public information, notification, and awareness for all travelers, including U.S. citizens, with regard to biometric collection pursuant to this rule.

Response: CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII. Besides this rule, additional information can be found on CBP’s website, in the TVS PIA, and in the CPE TVS Report.⁷⁶ Where airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP.⁷⁷ CBP provides notice to departing travelers at airport departure gates and travelers arriving at ports of entry through message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP or a stakeholder will be taking photos for identity verification purposes.⁷⁸ CBP also provides notice to the public regarding opt-out procedures for U.S. citizens.⁷⁹ CBP works with airlines, cruise

⁷⁶ *See* <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>; TVS PIA at 1; and CPE TVS Report at 1, 5-7.

⁷⁷ *See* CPE TVS Report at 6.

⁷⁸ *See* CPE TVS Report at 6.

⁷⁹ *See* CPE TVS Report at 6.

line operators, airports, and other port facilities to incorporate appropriate notices and processes into their current business models.⁸⁰ Additionally, signage posted at CBP's FIS area provides information to travelers on search procedures and the purpose for those searches.⁸¹ Upon request, CBP officers provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on CBP's biometric matching process, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.⁸² Current text for signs and tear sheets are also available on CBP's Biometrics Resources website, <https://www.cbp.gov/travel/biometrics/resources>.

Privacy information on the program such as SORNs and PIAs, including the TVS PIA and information on CBP's previous pilots during the development and testing of facial comparison technology, are published on the DHS Privacy website, <https://www.dhs.gov/privacy>. A link to the TVS PIA is provided on CBP's Biometric Privacy Policy website, <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>. Also available on CBP's Biometric Privacy Policy website is the CPE TVS Report.

In response to the 2020 GAO audit recommendations,⁸³ and as noted in the Status of Recommendation 1 in the Recommendations for Executive Action Table on the applicable GAO website,⁸⁴ CBP launched its updated biometrics website on September 1, 2020 (<https://www.cbp.gov/travel/biometrics>). The purpose of the site is to deliver information to the public and other stakeholder groups. The site provides a user-friendly communication channel for promoting facial comparison technology and biometrics

⁸⁰ See CPE TVS Report at 6.

⁸¹ See CPE TVS Report at 6-7.

⁸² See CPE TVS Report at 6.

⁸³ See GAO, GAO-20-568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (2020), available at <https://www.gao.gov/products/gao-20-568> (last visited May 16, 2025).

⁸⁴ See GAO, GAO-20-568, Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, Recommendations, Recommendations for Executive Action Table, <https://www.gao.gov/assets/gao-20-568.pdf> (last visited May 16, 2025).

information in a dynamic and interactive manner. As a testament to CBP's commitment to privacy protections, outlined in the DHS FIPPS, the CBP biometrics website includes the current locations using facial comparison technology, as well as information on how to request alternative screening and copies of CBP's privacy signage on display. The information provided, including a link to CBP's TVS PIA, is yet another tool CBP uses to ensure technology sustains and does not erode privacy protections.

Additionally, CBP has briefed the staff of the CBP Information Center to ensure the staff has the latest information to answer questions. CBP will continue to ensure that content is up to date on the CBP biometrics website, as required, and when substantive updates are made, CBP will provide new details to the CBP Information Center.

Furthermore, CBP regularly conducts periodic signage audits that include local CBP personnel to ensure signs are accurate and placed appropriately.⁸⁵ It is important to note that, unlike FIS areas, the airport departure areas are not managed by CBP personnel. However, CBP will continue to work with its airline/airport partners to ensure that privacy signage is available, on display, and reflective of current privacy messaging for travelers.

Comment: Additionally, some commenters stated that all signage and communication should clearly identify a contact and process for any traveler to file a grievance should the traveler feel that the traveler was improperly or unfairly treated during the biometric collection process.

Response: If a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information, (i.e., if the TVS finds a mismatch, false match, or no match) inquiries may be directed to CBP Information Center, Office of Public Affairs - MS1345, U.S. Customs and Border Protection, 1300 Pennsylvania

⁸⁵ See CPE TVS Report at 7.

Avenue, NW, Washington, DC 20229, or online at

https://help.cbp.gov/s/?language=en_US. Travelers may also contact the DHS Traveler

Redress Inquiry Program (DHS TRIP), 6595 Springfield Center Drive TSA-910,

Springfield, VA 22150-6901, or online at <https://www.dhs.gov/dhs-trip>, if they have

experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s).

Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. Further, an individual may submit

a Privacy Act amendment request to have their travel history record amended if they

believe there is incorrect or inaccurate information in their record(s). Privacy Act

amendment requests may be sent to privacy.cbp@cbp.dhs.gov.

CBP agrees that it is important to advise the traveling public of appropriate redress mechanisms if a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information. Nevertheless, CBP must be mindful of the limited space on the sign itself. Current signage language directs travelers to the CBP biometrics website for more information. The CBP biometrics website includes several additional links to additional resources such as information on the FOIA, the CBP Information Center and a link to the DHS website, <https://www.dhs.gov>. On the DHS website, the public can submit a DHS TRIP complaint as discussed above.

CBP will continue to keep the public informed regarding the use of facial comparison technology as it expands to additional locations.

Comment: One commenter requested additional information on exactly who will be targeted for this biometric collection.

Response: As discussed throughout this rule, upon the effective date of this final rule, collection of facial biometrics may be required from all aliens entering or exiting the United States, regardless of age, gender, race, or nationality.

Comment: One commenter indicated this rule fails to provide individuals with a choice or general awareness on whether travelers' personal information will be used to develop and/or train machines or algorithms.

Response: CBP has issued PIAs for many of the pilots that have tested facial comparison technology.⁸⁶ Furthermore, the relevant SORNs are clear that DHS/CBP may use biometrics for purposes of testing new technology and identity verification.⁸⁷

Comment: Two commenters noted that they had only just heard about this rule and that the previous administration did not want input from the public.

Response: DHS respectfully disagrees. In addition to following the legal requirements for providing notice to specifically seek input from the general public in accordance with the Administrative Procedure Act (APA), 5 U.S.C. 553(b), by publishing the proposed rule in the *Federal Register* on November 19, 2020, CBP also issued a press release,⁸⁸ In February 2021, in alignment with DHS's transparency efforts, DHS published another notice in the *Federal Register* to allow the public another opportunity to provide comments on the NPRM regarding the expansion of facial biometrics to

⁸⁶ See DHS/CBP/PIA-025 1:1 Facial Comparison Project, DHS/CBP/PIA-026 Biometric Exit Mobile Air Test, DHS/CBP/PIA-027 Southwest Border Pedestrian Exit Field Test, DHS/CBP/PIA-030 Departure Information Systems Test, and DHS/CBP/PIA-056 Traveler Verification Service. These PIAs are available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection> (last visited May 16, 2025).

⁸⁷ See DHS/CBP-006 Automated Targeting System SORN, 77 FR 30297, 30301-02 (May 22, 2012); and DHS/CBP-007 Border Crossing Information (BCI) SORN, 81 FR 89957, 89960-61 (Dec. 13, 2016). See also DHS/ALL-041 External Biometric Records (EBR) SORN, 83 FR 17829, 17831-32 (Apr. 24, 2018); DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) SORN, 85 FR 14955, 14957 (Mar. 16, 2020); DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, 73 FR 77778, 77780-81 (Dec. 19, 2008); and DHS/CBP-021 Arrival and Departure Information Systems (ADIS) SORN, 80 FR 72081, 72083 (Nov. 18, 2015). These SORNs are available at <https://www.dhs.gov/system-records-notices-sorns> (last visited May 16, 2025).

⁸⁸ CBP, National Media Release, CBP Enhances Biometrics for Non-U.S. Travelers Entering and Exiting the United States, Nov. 20, 2020, available at <https://www.cbp.gov/newsroom/national-media-release/cbp-enhances-biometrics-non-us-travelers-entering-and-exiting-united> (last visited May 16, 2025).

further secure and streamline the international travel process. 86 FR 8878 (Feb. 10, 2021). Furthermore, CBP issued a separate press release discussing the NPRM and reiterating that the comment period was reopened.⁸⁹

e. U.S. Citizen Opt-Out

Comment: A few commenters raised concerns about U.S. citizen options for opting out of using this biometric technology, including training of officers, signage and notification, alternative inspection methods, and authority to collect data.

Response: DHS disagrees with these comments. Pursuant to section 287(b) of the INA (8 U.S.C. 1357(b)), all U.S. citizens are subject to inspection upon arrival to and departure from the United States to confirm their identity and citizenship. However, as noted here and elsewhere throughout this final rule, U.S. citizens can voluntarily participate in the facial biometric process. As mentioned on the privacy signage, also available on <https://www.cbp.gov/travel/biometrics>, if a U.S. citizen does not wish to have a photograph taken, the U.S. citizen may see a gate agent or CBP officer to request alternative procedures for identity verification.

The alternative procedures implemented pursuant to this rule are intended to be similar to the existing process at entry today, in which a CBP officer physically examines the traveler's documentation to ensure the bearer is the true owner and scans the document to pull up the traveler's data for inspection. On exit, airline partners would then conduct manual identity verification using the travel document, as is done today with minimal impact to the boarding and exit process. If there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, the airline will contact CBP for additional

⁸⁹ CBP, National Media Release, CBP Reopens Comment Period Regarding Enhancements to Biometrics for non-U.S. Citizens Entering, Exiting United States, Feb. 9, 2021, available at <https://www.cbp.gov/newsroom/national-media-release/cbp-reopens-comment-period-regarding-enhancements-biometrics-non-us> (last visited May 16, 2025).

inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask the traveler questions to validate identity and citizenship. As mentioned above, every effort will be made to not delay or hinder travel; however, as the alternative procedures include a more manual process it may be slower than the automated process using facial comparison technology.

Prior to deploying facial comparison technology to ports of entry, CBP conducts extensive and on-going officer training, including emphasis on U.S. citizens being able to request to opt-out of having their photo taken and instead proceed through the traditional inspection process consistent with existing requirements for entry into the United States. Additionally, CBP sends reminder memos to the field offices to ensure compliance.

Comment: Commenters also raised concerns regarding the possibility of an eventual biometric collection mandate for all U.S. citizens.

Response: At this time CBP does not have plans to require U.S. citizens to be photographed when entering or exiting the United States as evidenced by DHS's withdrawal of the 2008 NPRM which would have proposed to require biometrics from U.S. citizens. *See* Withdrawal Notice (85 FR 73644).

f. Disability, Religious and Language Accommodations

Comment: A few commenters raised concerns surrounding religious and language accommodations, including the need for alternative processing for travelers with religious affiliations, disabilities, or limited English-language proficiency.

Response: CBP treats all international travelers with dignity, respect and professionalism while keeping the highest standards of security. For travelers with religious affiliations and/or disabilities, CBP policy generally allows for alternative processing on a case-by-case basis. These methods include fingerprint scans or requesting additional documents to establish identity and citizenship. On exit, the airline gate agent may conduct manual identity verification of travelers by using their travel

documents, as is performed for flights where biometric processing is not available, and may notify CBP to conduct further examination, if necessary. For example, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask the traveler questions to validate identity and citizenship.

CBP requires the full face to be viewable. As such, CBP may request that the individual adjust or remove religious headwear to the degree necessary for identification verification. Should religious headwear need to be removed, CBP endeavors to provide as much privacy as possible. During processing, if a traveler requires special consideration due to religion, cultural, or privacy concerns, CBP officers and managers should endeavor to reasonably accommodate the traveler's request.

CBP has long recognized the importance of effective and accurate communication between CBP personnel and the public they serve. Language and communication barriers can negatively affect interactions with the public, provision of services, and law enforcement activities. Ensuring effective communication with all persons facilitates the CBP mission. CBP has a protocol for the use of interpreters and translation services, which is triggered by a request for interpreters or language services.⁹⁰ Air carriers and airport authorities may also provide interpreters for travelers, typically through Airport Ambassadors. CBP also utilizes other means of interpretation and translation, including Agency employees certified to provide language services. Additionally, CBP developed an internal smartphone translation application, CBP Translate, to facilitate basic officer-

⁹⁰ See CBP, Language Access, <https://www.dhs.gov/publication/language-access-plan-us-customs-and-border-protection> (providing links to the DHS and CBP Language Access Plans) (last visited May 16, 2025).

traveler conversations. Privacy information about CBP Translate is provided in DHS/CBP/PIA-069 Privacy Impact Assessment for the CBP Translate Application (2021), available at <https://www.dhs.gov/publication/dhscbppia-069-cbp-translate-application> (last visited May 15, 2025).

Comment: One commenter expressed concern over requiring travelers to remove their face masks during the facial comparison process.

Response: The Centers for Disease Control and Prevention’s Order entitled “Requirement for Persons To Wear Masks While on Conveyances and at Transportation Hubs”⁹¹ has expired and most travelers no longer wear masks. However, CBP recognizes that some travelers still choose to wear masks and understands the concerns of those travelers. During both entry and exit, traveler identity must be verified, whether it is by a CBP officer or by a gate agent (on departure). To verify identity, it is necessary to see a person’s face, whether it is being viewed by a camera or by a person. An argument can be made that it takes less time for a camera to capture a photo and do a backend comparison than it does for a person to make the same comparison and decide whether or not the faces match. In that case, using facial comparison technology lessens the time a traveler has to be without wearing a mask.

As such, once at the primary inspection booth, CBP requires that all travelers momentarily lower their masks either to conduct the facial comparison match or to visually confirm that the traveler is the true bearer of the travel document. Requiring travelers to briefly remove their masks does not violate any laws. Upon departure, CBP defers to stakeholders, but does request that travelers pull their masks down as much as possible and ensure that no other facial obstructions (e.g., hats or glasses) are present. If CBP officers are present upon departure, CBP will request that travelers pull their masks

⁹¹ See 86 FR 8025 (Feb. 1, 2021).

down. Nevertheless, facial comparison technology continues to improve. For example, a 2020 DHS S&T study showed that systems are often able to correctly identify individuals with masks.⁹² CBP will continue to consider alternatives to mask removal using improved technology for those rare cases where travelers are still using masks.

g. Data Security, Retention, and Dissemination Concerns

Comment: Several commenters raised concerns surrounding data security, retention, and dissemination to include protecting the biometric data from breaches, cyberattacks, or insider threats, and implementing appropriate safeguards and storage protocols.

Response: CBP is committed to protecting all sensitive information in its possession, including mitigating, to the extent possible, the risk of data breaches from information systems containing PII. Privacy is implemented by design. It is ensured in this instance because data protection is built into the design, architecture, and implementation of the biometric technology, ensuring data protection through the architecture and implementation of the biometric technology. As further detailed below, there are four primary safeguards to secure traveler data: secure encryption during data storage and transfer; irreversible biometric templates; brief CBP retention periods; and secure storage.

- *Encryption:* CBP stores TVS information in secure CBP systems and temporarily in a secure virtual cloud environment.⁹³ CBP uses two-factor authentication and strong encryption to transfer the data between the camera, the TVS cloud matching

⁹² DHS S&T, News Release, Airport Screening While Wearing Masks? Facial Recognition Tech Shows up to 96% Accuracy in Recent Test, Jan. 4, 2021, available at <https://www.dhs.gov/science-and-technology/news/2021/01/04/news-release-airport-screening-while-wearing-masks-test> (last visited May 16, 2025); DHS S&T, Demographic Variation in the Performance of Biometric Systems: Insights Gained from Large-Scale Scenario Testing (2021), available at <https://www.dhs.gov/publication/demographic-variation-performance-biometric-systems> (last visited May 16, 2025).

⁹³ See TVS PIA at 26; CPE TVS Report at 15.

service, and CBP systems as well as for PII at rest (in storage). Moreover, just as CBP encrypts all biometric data at rest and in transit, CBP requires its approved partners under the TVS partner process to encrypt the data, both at rest and in transit.

- *Templates:* A biometric template is a digital representation of a biometric trait of an individual generated from a biometric image and processed by an algorithm. The template is usually represented as a sequence of characters and numbers.⁹⁴ For TVS, the secure biometric templates created from the photos cannot be reverse engineered to recreate a biometric image. The templates generated for the TVS are proprietary to a specific vendor's algorithm and cannot be used with other vendors' algorithms.

- *Retention periods:* The entirety of TVS is in the cloud.⁹⁵ For U.S. citizens, the biometric image is destroyed immediately following confirmation of U.S. citizenship, but no later than 12 hours only under specific circumstances.⁹⁶ If there is a system or network issue, photos will reside in an inaccessible queue for up to 12 hours and will be processed once the system and/or network connectivity is re-established and proper dispositioning (confirmation of U.S. citizenship) can occur. For all other travelers, CBP temporarily retains facial images in the internal cloud for no more than 14 days for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. Gallery photos of all air and sea travelers are purged from the TVS external cloud matching service no later than 12 hours after entry or departure. CBP's cloud service provider, using a configurable managed service, automatically deletes the data. Additionally, the data cache is in an encrypted form and the cloud service provider does not have the encryption keys. CBP does not create galleries for the land environment. Photos of aliens who are required to provide a

⁹⁴ See TVS PIA at 6, 26; CPE TVS Report at 15-16.

⁹⁵ See TVS PIA at 6; CPE TVS Report at 15.

⁹⁶ See TVS PIA at 9-10; CPE TVS Report at 11, 16.

biometric as well as those U.S. citizens who participate in CBP's Global Entry Program, are securely transferred from CBP's cloud service providers to DHS IDENT, and any successor systems.⁹⁷ Certain other federal agencies may access IDENT with the approval of DHS, if the purpose of their access is consistent with the applicable SORNs, which are available on the DHS website, <https://www.dhs.gov/system-records-notice-sorn>.⁹⁸ DHS retains certain records in IDENT for up to 75 years, which is necessary to support the holding of biometrics of subjects of interest in immigration and border management or law enforcement activities.⁹⁹

- *Access controls:* Only authorized CBP personnel and authorized representatives of approved CBP partners have access to the cameras, and only authorized CBP staff and cloud service provider personnel have access to the cloud database.¹⁰⁰ Although authorized cloud personnel may access the database, they do not have keys to decrypt the data. CBP access controls ensure only authorized access to the facial images. Initial TVS access is not activated for an individual without completion of the CBP Security and Privacy Awareness course.¹⁰¹ The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and TVS users are required to take the course annually.¹⁰² Furthermore, the cloud service provider selected for this initiative is required to adhere to the security and privacy controls

⁹⁷ See TVS PIA at 8-9.

⁹⁸ See TVS PIA at 22.

⁹⁹ See TVS PIA at 21.

¹⁰⁰ See TVS PIA at 26; CPE TVS Report at 15.

¹⁰¹ See TVS PIA 2 at 7; CPE TVS Report at 15.

¹⁰² See CPE TVS Report at 15.

required by NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (2011)¹⁰³ and the DHS Chief Information Officer.

CBP experienced a cybersecurity incident during a biometric pilot in 2019.¹⁰⁴ DHS OIG reviewed the incident to determine whether CBP ensured adequate protection of biometric data during the 2019 pilot.¹⁰⁵ In response to the 2019 cybersecurity incident, CBP has taken and continues to take robust measures to protect information systems containing PII. CBP response actions are detailed in CBP Comments to the Draft Report found in Appendix B to the Sept. 2020 DHS OIG Report regarding the incident.¹⁰⁶

In addition to the assessment of biometric exit stakeholders, discussed in more detail below, CBP is working with DHS S&T, Office of Test and Evaluation, to develop and execute a cybersecurity test plan that will ensure all required security controls are in place on existing hardware and software. Additionally, CBP has contracted with a third-party vendor to perform an adversarial assessment to identify and mitigate any cyber vulnerabilities.

Comment: Several commenters also suggested auditing stakeholders (such as port authorities, air carriers and sea carriers) to ensure compliance.

Response: CBP understood the need to build a system that all stakeholders within the travel continuum could participate in without building their own independent systems. To address these challenges and satisfy the Congressional mandate, CBP, as outlined above, is working closely with its partners to integrate biometrics with existing identity verification requirements to the extent feasible. CBP agrees that it needs to ensure that its

¹⁰³ Available at <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf> (last visited May 16, 2025).

¹⁰⁴ See DHS OIG, OIG 20-71, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot 5 (2020) (Sept. 2020 DHS OIG Report), available at <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf> (last visited May 16, 2025).

¹⁰⁵ Sept. 2020 DHS OIG Report at 5.

¹⁰⁶ Sept. 2020 DHS OIG Report at 22-23.

partners comply with and adhere to DHS and CBP privacy and security policies. To that end, CBP developed Business Requirements Documents, available on CBP's biometrics website at <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>, which partners sign and return to CBP as acknowledgement by the stakeholder that it agrees to all CBP terms and technical specifications as well as any other requirements as determined by CBP.¹⁰⁷

These business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP's facial comparison technology. CBP prohibits all approved partners such as airlines, airport authorities, or cruise lines and participating organizations (e.g., vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.¹⁰⁸ The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement.¹⁰⁹ In order to use TVS, private sector partners must agree to these Business Requirements.¹¹⁰

CBP comprehensively assesses compliance with DHS's security and privacy requirements on the part of CBP and CBP's partners. This includes security interviews with partner IT departments, security scans of biometric processing systems, and penetration tests of those systems. CBP has conducted 14 assessments thus far.¹¹¹ CBP

¹⁰⁷ CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

¹⁰⁸ CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

¹⁰⁹ CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

¹¹⁰ CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

¹¹¹ Information provided by CBP's Biometric Entry-Exit Strategic Transformation Admissibility and Passenger Programs office subject matter expert on January 4, 2024.

has not found any instances of stakeholders' retaining photos in violation of the Business Requirements Document.

CBP's cybersecurity resilience efforts, including the assessment of biometric exit stakeholders and adversarial assessment, align with Executive Order 14028, "Improving the Nation's Cybersecurity," 86 FR 26633 (May 17, 2021), which highlights the need to strengthen collaboration between the private sector and the Federal Government.

Furthermore, CBP is taking steps to promote data minimization and privacy protections by using an airline-generated alphanumeric unique ID (UID) to disassociate the biographic information associated with the new facial images. As CBP verifies the identity of the traveler, either through the automated TVS facial comparison process or manual officer processing, the backend matching service returns the "match" or "no-match" result, along with the associated unique identifier. There is no additional PII shared with industry partners, which minimizes harm to individuals should cybersecurity incidents occur. A UID is generated by either the travel agent, travel website hosting service, or the airline at the time of the reservation. The UID is comprised of a sequential number (which is only valid for the particular airline and the specific flight), plus the Record Locator, a six-digit code used to access additional information about the traveler.

Comment: Several commenters also suggested limiting forward dissemination.

Response: DHS discloses information sharing pursuant to the relevant SORNs, under the Privacy Act. As discussed above, these SORNs are available on the DHS website at <https://www.dhs.gov/system-records-notice-sorn>. DHS abides by all applicable confidentiality statutes and regulations that may limit the use and sharing of information about vulnerable populations including those covered by IIRIRA 110 (8 U.S.C. 1367) (Violence Against Women Act, T nonimmigrant visas, and U nonimmigrant visas); INA 244 (8 U.S.C. 1254a(c)(6)) and 8 CFR 244.16 (Temporary Protected Status); INA 245A (8 U.S.C. 1255a(c)(5)(A) and (B), LIFE Act, P.L. 106-553

§ 1104(c)(5) and 8 C.F.R. § 245a.2(t); 245a.3(n), and 8 C.F.R. § 245a.21) (Legalization under the LIFE Act); INA 210 (8 U.S.C. 1160(b)(6)(A) and (B)), 8 CFR 210.2(e) (Special Agricultural Workers); and 8 CFR 208.6 (Asylum, credible fear, and reasonable fear, and applicable by DHS policy to Refugee information).

Additionally, in accordance with DHS policy, CBP uses the DHS FIPPs¹¹² to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. DHS applies FIPPS-based protection to ensure that any forward dissemination is for a valid purpose consistent with the purpose for the original collection, is for a limited use consistent with the applicable SORN, and that privacy protections are adhered to. CBP's partnering stakeholders are also held to the same standards. For additional information on how CBP complies with the FIPPS, please see the page 15 of the CPE TVS Report.

DHS prioritizes data protection and security as part of its mission to protect the homeland and is cognizant of the serious impact that unauthorized disclosure of information could create for vulnerable populations. DHS acknowledges that the risk of a data breach is always technically possible, but DHS works tirelessly to minimize those risks and continues to safeguard its information from any unauthorized use. DHS's IDENT already contains controls so that only those individuals whose jobs require knowledge of information retained in IDENT (including facial images as discussed in the response in this section above at the bullet on *Retention Periods*) are able to access that data on a need-to-know basis. In addition, government employees accessing IDENT data must have a valid federal security or suitability clearance. Misuse of the data in IDENT is mitigated by requiring that IDENT users conform to appropriate security and privacy

¹¹² DHS, The Fair Information Practice Principles, <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles> (last visited May 16, 2025).

policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

Further, external connections must be documented and approved with both parties' signatures in an Interconnection Security Agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed. DHS OBIM is responsible for all PII associated with IDENT, and the Homeland Advanced Recognition Technology System (HART), the successor system to IDENT currently in development, whether the data is held in data centers or in a cloud infrastructure, and therefore imposes strict requirements for safeguarding PII.¹¹³ This includes adherence to the DHS 4300A Sensitive Systems Handbook,¹¹⁴ which provides implementation criteria for the rigorous requirements mandated by the DHS Information Security Program.

Additionally, DHS OBIM requires contracted cloud service providers to segregate IDENT and HART data from all other third-party data.¹¹⁵ All contracted cloud service providers must also follow DHS privacy and security policy requirements and must follow the Federal Risk and Authorization Management Program (FedRAMP)'s strict configurations, security assessments, authorizations, and continuous monitoring requirements.

h. Rulemaking Process – Comment Period

Comment: Several commenters raised concerns regarding the 30-day comment period and asserted that DHS did not provide sufficient time for public review. One

¹¹³ See HART PIA at 38-39.

¹¹⁴ DHS, DHS 4300A Sensitive Systems Handbook, Version 12.0 (Nov. 15, 2015), available at https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf (last visited May 16, 2025).

¹¹⁵ See HART PIA 38.

commenter also alleged that DHS's staggered issuance of interrelated rules (referencing the USCIS NPRM) created further difficulties for interested parties as commenters were prevented from determining how the rules interrelate within the comment periods for the related rules.

Response: Following the initial 30-day comment period, which closed on December 21, 2020, CBP, in alignment with DHS transparency efforts, and based on the previous comments received, re-opened the comment period for an additional 30 days to provide the public another opportunity to provide comments on the NPRM regarding the expansion of facial biometrics to further secure and streamline the international travel process.¹¹⁶ The second period was from February 10 to March 12, 2021.¹¹⁷ The combined comment periods amounted to 60 days. Although section 6(a)(1) of Executive Order 12866 and section 2(b) of Executive Order 13563 recommend as a general matter that agencies provide a minimum comment period of 60 days, the APA does not prescribe a minimum number of days necessary to allow for adequate comment. *See* 5 U.S.C. 553(b). Therefore, in accordance with the APA and the applicable Executive Orders, DHS set a 30-day comment period and further re-opened the comment period for an additional 30 days which reasonably provided the public with a meaningful opportunity to comment. Additionally, CBP notes that the USCIS NPRM has been withdrawn. 86 FR 24750 (May 10, 2021).

i. Rulemaking Process – Unauthorized official and other DHS authority concerns

Comment: Several commenters claimed that the rule was promulgated by an unauthorized official making the rule null and void.

¹¹⁶ 86 FR 8878 (Feb. 10, 2021).

¹¹⁷ 86 FR at 8878.

Response: It is unnecessary to discuss the merits of the appointments because the NPRM only proposed changes to DHS regulations and requested comments. It did not effectuate any change that would amount to a final action taken by DHS.

Comment: Some commenters alleged that the rule is a violation of the APA because the administration does not have the authority to issue regulations that go beyond the agency's statutory mandate or that CBP has misinterpreted Congress's directions regarding a biometric entry-exit program. The commenters also alleged that DHS's failure to substantiate a need for biometrics expansion conflicts with the requirements of the APA as the APA prohibits agency actions that are arbitrary, capricious or an abuse of discretion or unsupported by substantial evidence. *See* APA (5 U.S.C. 706(2)).

Response: DHS is not exceeding the statutory authorities as they currently exist. In accordance with the APA, DHS explicitly articulated both general and specific statutory authority for biometric collection including photographs, in the NPRM¹¹⁸, reiterates that authority in Section III.B. of this final rule, and disagrees with commenters that it does not have authority to promulgate this rulemaking. Additionally, DHS has provided extensive discussion of the need and purpose for this rulemaking pursuant to the APA requirements. For more information on the need for a biometric entry-exit program, see Section II.B. above.

j. Government Accountability and Oversight

Comment: Several commenters raised concerns regarding effective oversight activities, and accountability measures. Additionally, some commenters noted the importance of instituting uniform standards across the U.S. Government. One commenter supports the Homeland Security Advisory Council November 2020

¹¹⁸ *See* the NPRM, 85 FR at 74164 for more information regarding DHS' statutory authority to require biometrics.

findings¹¹⁹ and recommendations, including the establishment of a DHS Biometrics Oversight and Coordination Council.

Response: As the Biometric Entry-Exit Program is a congressionally mandated government program, there are several oversight processes to ensure compliance with civil rights and civil liberties. These processes include congressional hearings, congressionally mandated status update reports and responses to formal congressional inquiries, as well as audits from the GAO and OIG.

CBP participated in two congressional hearings, one in 2019¹²⁰ and in 2020,¹²¹ as well as responded to more than seven congressional inquiries since 2017 regarding CBP's use of facial comparison technology.

Additionally, CBP has published several reports that provide the public with information on how CBP is implementing the Biometrics Entry-Exit Program. For example, in August 2019, DHS provided the U.S. House of Representatives Committee on Homeland Security a comprehensive report on the program that included material on the operational and security benefits of the biometric entry-exit system., CBP and TSA's efforts to address privacy concerns and potential performance differential errors, and a comprehensive description of audits performed.¹²²

CBP has addressed the recommendations from two audits, both in 2020, one by GAO and one by DHS OIG. See Sections V.B.2.c and V.B.4.b and d, above. CBP is

¹¹⁹ See HSAC Biometrics Report.

¹²⁰ See *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies*, Hearing Before the H. Comm. on Homeland Sec., 116th Cong. (2019) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP), available at <https://docs.house.gov/meetings/HM/HM00/20190710/109753/HHRG-116-HM00-Wstate-WagnerJ-20190710.pdf> (last visited May 16, 2025).

¹²¹ See *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II*, Hearing Before the H. Comm. on Homeland Sec., 116th Cong. (2020) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP), available at <https://docs.house.gov/meetings/HM/HM00/20200206/110460/HHRG-116-HM00-Wstate-WagnerJ-20200206.pdf> (last visited May 16, 2025).

¹²² See DHS, TSA and CBP: Deployment of Biometric Technologies Report to Congress (2019) is posted in the docket for this rulemaking.

aware of the DHS OIG report on its September 2023 audit, entitled “DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs.”¹²³ DHS OIG identified four recommendations; two for the Office of Strategy, Policy, and Plans to update and finalize internal DHS strategic plans and a department-wide policy for biometric collection in all transportation modalities and two recommendations for the Undersecretary for Management to update and finalize the DHS biometric implementation plan (roadmap) and for the Executive Steering Committee to continue the working group to develop a transition plan to integrate CBP’s biometric entry-exit system with OBIM’s HART system. Although none of these recommendations is directly specific to this rulemaking, CBP takes biometric capabilities seriously and is dedicated to work cooperatively with DHS to provide critical input regarding an overall management strategy to acquire and deploy a biometric solution that meets Department needs, particularly regarding integration of CBP’s biometric entry-exit system with HART (the successor system to IDENT, as noted elsewhere).

Furthermore, CBP complies with the requirements of the Privacy Act, as well as all DHS and Government-wide policies. In accordance with DHS policy, CBP uses the FIPPs to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. CBP’s partnering stakeholders are also held to the same standards. For additional information on how CBP complies with the FIPPs, please see page 15 of the CPE TVS Report.

Also, the business requirements implemented by CBP with its partners govern the retention and use of the facial images collected using CBP’s facial comparison technology. The Business Requirements Documents are available on CBP’s biometrics

¹²³ DHS OIG, OIG 23-58, DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs (2023), available at <https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-58-Sep23.pdf> (last visited May 16, 2025).

website at <https://www.cbp.gov/travel/biometrics/biometric-privacy-policy>. CBP prohibits its approved partners such as airlines, airport authorities, or cruise lines and participating organizations (e.g., vendors, systems integrators, or other third parties) from retaining the photos they collect under this process for their own business purposes.¹²⁴ The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement.¹²⁵ In order to use TVS, private sector partners must agree to these Business Requirements.¹²⁶

Several DHS Offices and Programs also have oversight of CBP activities. For example, CBP collaborates regularly with the DHS Privacy Office to ensure compliance with privacy laws and policies. The DHS Privacy Office commissioned the DHS Data Privacy and Integrity Advisory Committee (DPIAC) to advise DHS on best practices for the use of facial comparison technology. The DHS DPIAC published its report on February 26, 2019.¹²⁷ CBP has implemented or is actively working to implement all of the DHS DPIAC recommendations.

Additionally, in June 2019, the Privacy and Civil Liberties Oversight Board (PCLOB) started an ongoing oversight project to review the use of facial comparison technology in aviation security, with the goal of informing policymakers and the public about these technologies, their uses, and their implications for security, privacy, and civil

¹²⁴ CBP Biometric Air Exit Business Requirements 10; CBP Biometric Sea Entry-Exit Business Requirements 10.

¹²⁵ *Id.*

¹²⁶ CBP Biometric Air Exit Business Requirements 8; CBP Biometric Sea Entry-Exit Business Requirements 8.

¹²⁷ DHS DPIAC, Report 2019-01: Privacy Recommendations in Connection with the Use of Facial Recognition Technology (2019), available at https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf (last visited May 19, 2025).

liberties.¹²⁸ CBP hosted the PCLOB for a tour of biometric processes at

Atlanta/Hartsfield International Airport on January 15, 2020.¹²⁹

Furthermore, CBP works closely with DHS S&T, OBIM and NIST on technical standards and system performance. Additionally, CBP is a member of the DHS Biometric Capabilities Executive Steering Committee (BC-ESC), which continues to meet quarterly.¹³⁰ The mission of the BC-ESC is to provide effective governance, oversight, coordination, and guidance to all DHS and component-level programs that are developing and/or providing biometric capabilities in support of DHS mission objectives.¹³¹ It serves as a forum for cross-component collaboration and the sharing of biometric challenges, needs, concepts, best practices, plans, and efforts.

Although CBP's Biometric Entry-Exit Program does have sufficient oversight and accountability mechanisms, CBP is committed to transparency in its use of facial comparison technology and welcomes the opportunity to engage with Congress on legislative enhancements and to provide technical assistance, as necessary. CBP will ensure compliance with any new applicable legislation or regulations passed.

Comment: One commenter suggested that Congress pass an ethics bill prior to using facial comparison technology. One commenter suggested the United States needed a Cyber Bill of Rights.

¹²⁸ See PCLOB, Press Release, "From Booking to Baggage Claim:" PCLOB to Examine Use of Facial Recognition and Other Biometric Technologies in Aviation Security: Board Announces Three New Oversight Projects, June 26, 2019, available at https://documents.pclob.gov/prod/Documents/EventsAndPress/eb140554-4fc7-4700-88d2-197d7fe45770/New%20projects%20announcement%20June_25_%202019%20Final.pdf (last visited May 19, 2025); and PCLOB, Current Oversight Projects, <https://www.pclob.gov/OversightProjects> (last visited May 19, 2025).

¹²⁹ See *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II, Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. (2020) (statement of John P. Wagner, Deputy Exec. Assistant Comm'r, Off. of Field Operations, CBP at 9), available at <https://docs.house.gov/meetings/HM/HM00/20200206/110460/HHRG-116-HM00-Wstate-WagnerJ-20200206.pdf> (last visited May 19, 2025).

¹³⁰ See HSAC Biometrics Report 23.

¹³¹ See HSAC Biometrics Report 23.

Response: Comments suggesting Congressional action are outside the scope of this rulemaking. However, CBP will ensure compliance with any and all new applicable legislation passed by Congress.

Comment: Several commenters referenced specific abuse or misuse of power concerns. Some commenters mentioned alleged human rights violations committed by CBP and ICE. The commenters were concerned generally with CBP and ICE abuses, including a concern that this rule would open the door for further abuses of power and human rights violations.

Response: As documented in the DHS Core Values,¹³² DHS employees, including those of CBP, execute the duties and responsibilities entrusted to the agency with highest ethical and professional standards. Each DHS employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws, and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the Code of Federal Regulations as well as the implementing standards in supplemental agency regulations. *See* 5 CFR part 2635. Furthermore, CBP officers and agents follow the CBP Standards of Conduct.¹³³ Section 3.1 of the CBP Standards of Conduct specifically states, “The conduct of CBP employees must reflect the qualities of integrity and loyalty to the United States; a sense of responsibility for the public trust; courtesy and promptness in dealing with and serving the public; and a standard of personal behavior that reflects positively upon, and will be a

¹³² DHS, Core Values, <https://www.dhs.gov/core-values> (last visited May 19, 2025).

¹³³ CBP, Directive 51735-013B, Standards of Conduct (2020), available at https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf (last visited May 19, 2025).

credit to, both CBP and its employees.”¹³⁴ Section 7.11.2 further provides, “Employees will not make abusive, derisive, profane, or harassing statements or gestures, or engage in any other conduct evidencing hatred or invidious prejudice to or about another person or group on account of race, color, religion, national origin, sex, sexual orientation, age, or disability.”¹³⁵ The safety of CBP employees and the public is paramount during CBP operations.

Alleged violations by CBP or ICE officers or agents are outside the scope of this rulemaking.¹³⁶

k. Accuracy, General Bias, and Misidentification Concerns

Comment: Several commenters raised concerns regarding the accuracy, reliability, and potential bias of facial comparison technology, particularly its impact on specific demographic groups.

Response: DHS is aware of several NIST studies on the use of facial comparison technology and DHS continues to monitor the scientific community studies, particularly those of NIST, on applicability. The NIST FRVT Demographic Effects Report, which used CBP data to reach its conclusions,¹³⁷ noted that because different algorithms

¹³⁴ CBP, Directive 51735-013B, Standards of Conduct 1 (2020), available at https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf (last visited May 19, 2025).

¹³⁵ *Id.* at 11.

¹³⁶ Although outside the scope of this rulemaking, DHS notes the launch of the Office of the Immigration Detention Ombudsman (OIDO), a new and independent office within DHS as mandated by Congress. *See* section 106 of the Consolidated Appropriations Act, 2020, Pub. L. 116-93, 133 Stat. 2317, 2505 (amending section 405 of the Homeland Security Act (6 U.S.C. 205)). OIDO is an independent office within DHS and is not a part of ICE or CBP. OIDO’s role is to assist individuals with complaints about the potential violation of immigration detention standards or misconduct by DHS (or contract) personnel; provide independent oversight of immigration detention facilities, including conducting unannounced inspections and reviewing contract terms for immigration detention facilities and services; and serve as an independent office to review and resolve problems stemming from the same. *See* sec. 405(a)-(b) of the Homeland Security Act (6 U.S.C. 205(a)-(b)); DHS, Office of the Immigration Detention Ombudsman, <https://www.dhs.gov/office-immigration-detention-ombudsman> (last visited May 19, 2025).

¹³⁷ *See* DHS/OBIM/PIA-005, Privacy Impact Assessment for the Office of Biometric Identity Management (OBIM) - National Institute of Standards of Technology (NIST) Data Transfer 4-5 (2022), available at <https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards> (last visited May 19, 2025). *See also* TVS PIA at 22.

perform better or worse in various circumstances, “policy makers, face recognition system developers, and end users should be aware of these differences and use them to make decisions and to improve future performance.” NIST FRVT Demographic Effects Report 3.

To ensure higher accuracy rates, as well as efficient traveler processing, CBP uses high performing cameras, proper lighting, and image quality controls. CBP then compares traveler photos to a very small gallery of high-quality images that those travelers already provided to the U.S. Government to obtain a passport or visa using a high-quality facial comparison algorithm. CBP builds the galleries of photographs based on where and when a traveler will enter or exit. If CBP has access to advance information, CBP will build galleries of photographs based on upcoming flight or vessel arrivals or departures. CBP uses a commercial face comparison algorithm from a developer that participates in the NIST Face Recognition Technology Evaluation (FRTE) 1:N.¹³⁸ The NIST Face Recognition Vendor Test (FRVT) Demographic Effects Report, published in 2022, shows a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors and undetectable false positive differentials. Since many of the performance rates specified in the report would not be acceptable for use in CBP operations, CBP does not use them. Additionally, NIST noted, “Some developers supplied identification algorithms for which false positive differentials are undetectable” (NIST FRVT Demographic Effects Report 8). The most recent NIST FRTE 1:N demonstrates that the face comparison algorithm developer selected by CBP is capable of high performance, ranking within the top five in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP.

¹³⁸ NIST FRVT Demographic Effects Report 1, 8, 26.

The NIST performance metrics described in the NIST FRVT Demographic Effects Report are consistent with CBP operational performance metrics for entry-exit. CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. As mentioned in the CBP: Evaluating Possible Bias document included in the docket for this rulemaking, docket number [USCBP-2020-0062], CBP has conducted extensive statistical analysis (chi squared independence tests) to determine whether traveler demographics (age, sex, and nationality) affect facial comparison match rates.¹³⁹ CBP does not collect race/ethnicity information, and this information is not included in the APIS manifest. As a result, CBP uses citizenship as a proxy for this data. Using citizenship or country of birth as a proxy for race is consistent with industry standards as evidenced by the NIST FRVT Demographic Effects Report, which notes, "While country-of-birth information may be a reasonable proxy for race in these countries, it stands as a meaningful factor in its own right particularly for travel-related applications of face recognition." NIST FRVT Demographic Effects Report 1-2.

Additionally, CBP continually monitors algorithm performance and technology enhancements. As mentioned in CBP: Evaluating Possible Bias, the performance of CBP's TVS continues to improve over time due to technical, operational, and procedural advancements including threshold adjustments and testing multiple vendors.¹⁴⁰ CBP has enhanced the photo selection process used to build the galleries, which reduces the number of travelers with no photos and improves the accuracy of the system. Additionally, CBP has enhanced the manner in which the galleries are populated, ensuring that the information included in the flight manifest is used to its maximum

¹³⁹ CBP, CBP: Evaluating Possible Bias (2020), available at <https://downloads.regulations.gov/USCBP-2020-0062-0003/content.pdf> (last visited May 19, 2025).

¹⁴⁰ CBP, CBP: Evaluating Possible Bias (2020), available at <https://downloads.regulations.gov/USCBP-2020-0062-0003/content.pdf> (last visited May 19, 2025).

potential to include more, higher-quality photographs. There have also been software changes to the cameras to allow travelers posing for the photos to receive visual feedback. Furthermore, as CBP continues and expands its usage of TVS, personnel using the technology become more aware of the optimal camera positions to ensure better images and increase the traveler throughput. Some cameras are also now equipped with multiple lenses to capture images for various angles, which may increase photo quality depending on the height of the traveler. These advancements have been instrumental in minimizing occurrences of no matches, mismatches, and false matches.

CBP is also aware of several other tests, studies, and articles on the use of facial comparison technology. While informative, these studies do not evaluate the specific algorithm that CBP is using and as such cannot be used to draw conclusions about CBP's biometric entry-exit program.

Comment: Some commenters said that facial comparison technology should not be implemented until it is 100% accurate or until courts have shown that it is as effective as fingerprints for determining validity.

Response: DHS disagrees. No system or biometric technology, not even widely used fingerprints, is 100% accurate. In 2004, NIST found that “the best system was accurate 98.6 percent of the time on single-finger tests, 99.6 percent of the time on two-finger tests, and 99.9 percent of the time for tests involving four or more fingers. These accuracies were obtained for a false positive rate of 0.01 percent.”¹⁴¹ NIST conducted another study in 2020 that found contact device match accuracy is generally better than 99.5% when scanning multiple fingers.¹⁴² Fingerprint image quality may be affected by

¹⁴¹ NIST, News Release, NIST Study Shows Computerized Fingerprint Matching Is Highly Accurate, July 6, 2004, available at <https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerized-fingerprint-matching-highly-accurate> (last visited May 19, 2025).

¹⁴² See NIST, News Release, NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech, May 19, 2020, available at <https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech> (last visited May 19, 2025).

demographic factors. Operationally it is commonly observed that subject age, race, sex, and occupation often contributes to fingerprint image quality. For example, those with dry fingers due to the natural aging process as well as those with finer ridge structure specific to certain demographic groups may have poorer fingerprint match performance. There is also an occupation effect, in that people who work with their hands, such as brick layers, have matching issues. However, there are no detailed analysis reports that show how these image quality effects translate into fingerprint match performance.

Additionally, biographic systems are not 100% accurate either. As mentioned in the preamble, often there are errors or incomplete data. For example, the U.S. government may have the name and date of birth but not the passport number. The use of biographic data alone leads to a very high rate of mismatches, as dozens of people often have the exact same name and date of birth. The use of biometrics solves this problem by effectively and efficiently confirming a traveler's identity. Nevertheless, biometric algorithms should be framed against human matchers, not *100% perfect matching*, which is an impossibility. When comparing biometric matching to a human manual identity verification process, biometrics is a clear improvement and gets the process significantly closer to 100% than without biometric matching.¹⁴³ CBP is unaware of any legal requirement to show that facial comparison is the same as fingerprints for determining validity.

Comment: Two commenters expressed concern that facial comparison technology could be susceptible to imposter or spoof attacks.

Response: Even as technology advances, CBP is mindful of potential imposter or spoof attacks. CBP mitigates this risk through algorithm enhancements and its biometric

¹⁴³ See David White et al., Passport Officers' Errors in Face Matching, PLoS ONE 9(8): e103510 (2014), <https://doi.org/10.1371/journal.pone.0103510> (last visited May 19,2025).

approach using the gallery concept. CBP knows whom to expect to be on the flight based on the advance passenger information. Travelers, to include imposters, who are not expected on the flight would not match to the gallery.

Additionally, CBP mitigates spoof and imposter risk by ensuring that those utilizing the technology are appropriately trained to detect these attacks. CBP officers using the technology upon entry have several tools at their disposal, to include facial comparison technology, to identify imposters. Additionally, CBP officers undergo extensive training prior to starting the job, including specific tactics, techniques, and procedures for identifying imposters. For example, CBP has used Eye-dentify, which is an imposter detection training technology.¹⁴⁴ Additionally, CBP's Carrier Liaison Program provides carrier staff with training on U.S. entry requirements, human trafficking, traveler assessment, fraudulent document detection and impostor identification using state-of-the-art document examination material, equipment, and training tools.¹⁴⁵

Comment: Commenters requested additional information regarding CBP's mismatch rate, the outcome of potential misidentification and redress opportunities.

Response: As discussed in DHS's TSA and CBP: Deployment of Biometric Technologies Report to Congress, CBP's Biometric Air Exit KPPs mandate that the system's TAR must equal or exceed 97 percent of all in-scope travelers (as previously defined by 8 CFR 215.8 and 235.1) and that the system's FAR must not exceed 0.1 percent of all in-scope travelers.¹⁴⁶ The estimated TAR based on the internal CBP

¹⁴⁴ See DHS S&T, Snapshot: Customs and Border Protection Officers Leverage S&T-Developed Imposter Detection Training Tech to Maximize Officer Performance, <https://www.dhs.gov/science-and-technology/news/2020/02/25/snapshot-cbp-officers-leverage-st-developed-imposter-detection-training-tech> (last visited May 19, 2025).

¹⁴⁵ See CBP, Carrier Liaison Program Overview, <https://www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog> (last visited May 21, 2025).

¹⁴⁶ DHS, TSA and CBP: Deployment of Biometric Technologies Report to Congress 29-30 (2019), is posted in the docket for this rulemaking.

analysis is at least 98% for all travel modes. The estimated FAR based on the internal CBP analysis is 0.02 percent, which is within the established KPP target of less than 0.1 percent. Regarding false non-matches or false negatives, NIST states, “False negative error rates vary strongly by algorithm, from below 0.5% to above 10%. For the more accurate algorithms, false negative rates are usually low with average demographic differentials being, necessarily, smaller still.” NIST FRVT Demographic Effects Report 7. Moreover, “In cooperative access control applications, false negatives can be remedied by users making second attempts.” NIST FRVT Demographic Effects Report 3.

Additionally, while one commenter calculated the false non-match or false negative rate “by subtracting the true acceptance rate from 1,” NIST’s report indicates that “that definition is naïve in that it assumes every traveler was photographed. It ignores instances of failure-to-capture, and also cases where travelers are photographed, not matched, and then make further attempts.” NIST, NISTIR 8381, FRVT Part 7: Identification for Paperless Travel and Immigration 8 (2021) (NIST 2021 FRVT Report), available at <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pdf> (last visited May 15, 2025).

There are several factors that could contribute to travelers not matching to the gallery. For example, whether a traveler has a photo in the gallery and how many photos of the traveler are in the gallery are two main factors. Some of the reasons why a traveler may not have a photo staged in the gallery include: first-time travelers to the United States entering the country under the Visa Waiver Program (VWP), travelers on military orders, and travelers whose flight manifest data was incorrect. As noted in the NIST 2021 FRVT Report press release, “performance improves dramatically if the database contains multiple images of a passenger. The database gallery can contain more than one image of a single passenger. When an average of six prior images of a passenger are in

the gallery, then all algorithms realize large gains.”¹⁴⁷ Additionally, on exit, airline staff may choose to process travelers without having a photo taken. Physical changes, such as facial hair, hair style, make-up, and weight fluctuation do not affect a traveler’s ability to successfully match to a photo in the gallery. Changes to bone structure, for example a cosmetic surgery, may affect matching; however, in those instances CBP or the airline agent may use traditional inspection processes consistent with existing requirements for entry and exit.

Prior to deploying facial comparison technology to ports of entry, CBP conducts extensive officer training, including mismatch, false match, or no match procedures. As discussed in the rule, in the event of a mismatch, false match, or no match CBP may use alternative means to verify the traveler's identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler's document is performed. On entry, the CBP officer may continue to conduct additional screening or request fingerprints (if appropriate) to verify identity. Each inspection booth at entry is equipped with a fingerprint reader. At departure, the airline partner may conduct a manual review of the travel document (i.e., scanning a boarding pass and checking a traveler’s passport). If there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, the airline will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship.

In accordance with its statutory authority, CBP uses the totality of information available, to include the results of a facial comparison match, to make admissibility

¹⁴⁷ NIST, Press Release, NIST Evaluates Face Recognition Software’s Accuracy for Flight Boarding, July 13, 2021, available at <https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding> (last visited May 21, 2025).

decisions and take any law enforcement actions. Facial comparison alone does not determine admissibility. Nevertheless, if a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information, (i.e., if the TVS finds a mismatch, false match, or no match) inquiries may be directed to CBP Information Center, Office of Public Affairs - MS1345, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW., Washington, DC 20229, or online at https://help.cbp.gov/s/?language=en_US. Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 6595 Springfield Center Drive TSA-910, Springfield, VA 22150-6901, or online at <https://www.dhs.gov/dhs-trip>, if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. These mechanisms allow any errors, if they occur, to be rectified.

Individuals seeking notification of and access to biometric information contained in the TVS, or seeking to contest the results of the biometric matching process may gain access to certain information in the TVS by filing a Privacy Act access request by emailing privacy.cbp@cbp.dhs.gov or a Freedom of Information Act (FOIA) request online at [foia.gov](https://www.foia.gov) or <https://www.securerelease.us/>, or by mailing a request to: FOIA Officer, U.S. Customs and Border Protection, 90 K Street, NE, Washington, D.C. 20229, Fax Number: (202) 325-0150.¹⁴⁸ All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for

¹⁴⁸ For more information, see DHS, FOIA Contact Information, <https://www.dhs.gov/foia-contact-information> (last visited May 21, 2025).

information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

Comment: Several commenters also stated that this rule was premature prior to NIST issuing a final report on the performance of CBP's Biometric Exit Program.

Response: CBP is committed to implementing the biometric entry-exit mandate in a way that provides a secure and streamlined travel experience for all travelers, and CBP will continue to partner with NIST and use NIST research to ensure the continued optimal performance of the CBP face comparison service.¹⁴⁹ The NIST 2021 FRVT Report demonstrates that the current biometric facial comparison technology passes the threshold for use in CBP's Biometric Exit Program, based on computer-focused simulations.

l. Under 14 Children: Privacy, Authorities, and Accuracy Concerns

Comment: Several commenters raised concerns regarding collecting biometrics on minors specifically as it relates to violating privacy rights, CBP's authority to do so, the potential for misidentification due to lower accuracy rates, reliability, and potential bias of facial comparison technology, particularly its impact on specific demographic groups, and the outcome of potential misidentification. One commenter expressed concern over the rule's lack of information regarding how CBP will collect biometrics from small children as well as a lack of data that supports CBP claims that biometrics collection on children would actually combat trafficking. Two commenters mentioned that children

¹⁴⁹ See, e.g., DHS/OBIM/PIA-005 Office of Biometric Identity Management (OBIM)-National Institute of Standards of Technology (NIST) Data Transfer 3-5 (2022), available at <https://www.dhs.gov/publication/dhsobimpia-005-office-biometric-identity-management-obim-national-institute-standards> (last visited May 21, 2025).

are unable to consent to biometric collection and stated CBP should require parental consent similar to trusted traveler programs.

Response: Modality, age, and frequency of collection are all significant factors to consider when discussing accuracy associated with biometric matching of children. DHS does not necessarily believe that these factors render the act of biometrics collection less accurate or unnecessary for this population. Instead, DHS believes that to accurately address the changing nature of children's biometrics, DHS should collect their biometrics at shorter intervals. The Department of State tacitly recognizes the same principle in issuing passports for individuals under the age of 16, which are only valid for 5 years, whereas passports for individuals aged 16 and older are valid for a period of 10 years.¹⁵⁰ In any case, these validity periods and collection practices do not render the biometric collection inaccurate; the photograph of the child is accurate the day it is collected, but over time the usefulness of any given photograph decreases. DHS recognized this as an issue and this is one of the reasons why DHS intends to collect biometrics upon entry into and exit from the United States.

DHS disagrees with commenters that removing age restrictions violates the INA. DHS interprets section 287(f)(1) of the INA (8 U.S.C. 1357(f)(1)) to require photographs and fingerprints from aliens 14-years or older in removal proceedings, but that authority does not prohibit the collection from those younger than 14 as authorized by other laws. The language of the statute is silent regarding collecting biometrics from those under the age of 14 outside of enforcement proceedings, as it explicitly states, "the Commissioner shall provide for the fingerprinting and photographing of each alien 14 years of age or older against whom a proceeding is commenced" under section 240 of the INA (8 U.S.C. 1229a). INA 287(f)(1) (8 U.S.C. 1357(f)(1)). In addition, DHS is authorized to take and

¹⁵⁰ 22 CFR 51.4(b).

consider evidence (including biometrics) concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and the administration of DHS. *See* INA 287(b) (8 U.S.C. 1357(b)). Accordingly, DHS is authorized under the INA to collect biometrics on individuals under the age of 14.

DHS abides by all relevant privacy laws, regulations, and policies in collection of biometric information for individuals, including children. DHS disagrees that adding a biometrics requirement constitutes subjecting children to additional scrutiny or is inappropriate due to their inability to consent. CBP's responsibilities, regardless of age, gender, race and nationality, include ensuring the interdiction of persons illegally entering or exiting the United States, facilitating, and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States. *See* sec. 411(c) of the Homeland Security Act (6 U.S.C. 211(c)). Instead of verifying a child's identity using a manual review of travel documents, CBP will use facial comparison technology for identity verification at the border.

Not only will the facial comparison technology be used to determine and verify identity, but it will also support CBP efforts to ensure the safety of everyone crossing the border, including children. Typically, fraud schemes that DHS encounters involve adults and unrelated children posing as family units to DHS authorities. *See* John Davis, "Border Crisis: CBP Fights Child Exploitation," *Frontline Magazine*, Dec. 16, 2019, <https://www.cbp.gov/frontline/border-crisis-cbp-fights-child-exploitation> (last visited May 15, 2025). Nevertheless, minors can travel in and out of the United States without either one of their parents. To ensure the safety of children, CBP strongly recommends, but does not legally require, a notarized written consent letter from both parents. Since

FY 2019, CBP processed over 35 million children under the age of 14 at ports of entry, many without parents present.¹⁵¹ Minors require parental consent when applying for CBP's Trusted Traveler Programs as the programs are voluntary, and CBP requires consent for participation in all voluntary programs.

To take the photos of travelers, including children, CBP will not physically touch them. CBP may provide verbal instructions to the travelers to stand at a certain distance from the camera. Additionally, many cameras at CBP's primary inspection booths can be adjusted by the CBP officer to allow the CBP officer to place the camera in the optimal position to capture a high-quality image without touching the traveler. If CBP is unable to position the traveler to take a photo or in the event of a mismatch, false match, or no match, CBP may use alternative means to verify the traveler's identity and ensure that the traveler is not unduly delayed. If the system fails to match a traveler, then a manual review of the traveler's document is performed. This rule does not authorize the collection of other biometrics such as fingerprints on individuals younger than 14.

m. Surveillance

Comment: Several commenters raised concerns regarding the collection of photos being used for surveillance purposes, either by CBP or other U.S. Government Agencies that may have access to CBP data. Several commenters noted that use of facial comparison technology could support or lead to a police or carceral state. Several commenters noted that CBP could not be trusted with the technology as other government agencies have been criticized for using such technology to track journalists and protestors.

¹⁵¹ Information provided by CBP's Biometric Entry-Exit Strategic Transformation Admissibility and Passenger Programs Office, Office of Field Operations, subject matter expert on January 24, 2024.

Response: CBP's Biometric Entry-Exit Program will not utilize the facial images submitted for widespread surveillance as the commenters suggest. Biometric entry-exit is not a surveillance program. The Biometric Entry-Exit Program uses facial comparison technology to ensure a person is whom the person claims to be and is the bearer of the passport that is presented. This technology provides a seamless way for in-scope travelers, as described in the rule, to meet the requirement to provide biometrics upon arrival and departure from the United States. Travelers are aware their photos are being taken and U.S. citizens have the ability to request alternative procedures as described in the rule. CBP uses facial comparison technology only where a current identity check already exists. CBP uses only photos collected from cameras deployed specifically for this purpose and does not use photos obtained from closed-circuit television or other live or recorded video. The cameras in support of CBP's Biometric Entry-Exit Program are clearly visible to all travelers. Additionally, CBP works closely with partner carriers and airport authorities to post privacy notices and provide tear sheets for affected travelers and members of the public in close proximity to the cameras and operators, whether the cameras are owned by CBP or the partners.

Consistent with regulatory requirements, photos of aliens who are required to provide a biometric are securely transferred to DHS's IDENT.¹⁵² In the future, DHS intends to store these photos in IDENT's successor system, HART.¹⁵³ Certain other federal agencies and foreign partners may access these photos with the approval of DHS, if the purpose of their access is consistent with applicable SORNs.¹⁵⁴

¹⁵² TVS PIA at 8.

¹⁵³ HART PIA at 2.

¹⁵⁴ IDENT PIA at 3-5; HART PIA at 30.

DHS OBIM is the lead designated provider of biometric identity services for DHS and manages IDENT.¹⁵⁵ As IDENT contains data from a variety of sources, collected for a variety of uses, DHS has instituted necessary controls so that only those individuals with a need to know are able to access that data.¹⁵⁶ Further, being an authorized user of IDENT does not provide automatic access to all of an individual's IDENT records. IDENT has a robust set of access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections.¹⁵⁷ For example, organization-level data filtering is applied to encounter data, which allows for certain data (for example, asylum data) to be protected so that only approved organizations will be able to access the data. DHS sets the appropriate data filtering and access restrictions consistent with privacy and confidentiality laws and policies. DHS will continue to follow the latest technologies and trends with regard to protecting all data, whether it is biometric or biographic, in an effort to prevent any breach.

Misuse of the data in IDENT is mitigated by requiring that IDENT users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems.¹⁵⁸ Also, DHS conducts a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. Further, external connections must be documented and approved with both parties' signatures in an interconnection security agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

¹⁵⁵ DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) SORN, 85 FR 14955 (Mar. 16, 2020). *See* DHS, Office of Biometric Identity Management, <https://www.dhs.gov/obim> (last visited May 21, 2025).

¹⁵⁶ *See* IDENT PIA and Appendices.

¹⁵⁷ IDENT PIA at 27-28.

¹⁵⁸ IDENT PIA at 30.

DHS has policies in place to prevent improper sharing or unauthorized use of any data and nothing in this rule changes those policies.¹⁵⁹ IDENT maintains an audit record in the database for each system message sent to an external agency. Audit logs are maintained by OBIM's System Operations and Maintenance Branch. Access to audit logs is limited strictly to core System Operations and Maintenance Branch personnel. The audit log data are backed up regularly as part of the overall IDENT database backup and archiving process.

Comment: One commenter also expressed concern that technologies used in the United States could be adopted by other countries for surveillance as well.

Response: Regarding technologies used in the United States being adopted by other countries, CBP has no control over technologies adopted by other nations, therefore that issue is outside the scope of this rulemaking.

n. Violations of Constitutional Rights

Comment: Several commenters raised concerns regarding the impact of facial comparison technology to individuals' First, Fourth, Fifth, and Fourteenth Amendment rights. Specifically, commenters are concerned that the use of facial comparison technology will deter individuals from engaging in constitutionally protected activities, limit the right to travel, and violate the Fourth Amendment's protection against unreasonable searches of the people.

Response: DHS disagrees with these comments. DHS is not violating the Constitution of the United States with the changes made in this rule. As described in Section II of this preamble and clearly laid out in the NPRM, DHS has both general and

¹⁵⁹ See IDENT PIA at 27; HART PIA at 31.

specific statutory authority to collect or require submission of biometrics in its administration of the immigration laws.¹⁶⁰

Comment: Some commenters raised concerns about violations of the First Amendment protections for religion.

Response: Regarding the First Amendment, specifically, DHS will use facial comparison technology in the administration of immigration laws, not to curtail any of the freedoms afforded in the First Amendment. For travelers with religious affiliations, CBP policy generally allows for alternative processing to accommodate a traveler on a case-by-case basis. These methods include fingerprint scans or requesting additional documents to establish identity and citizenship. On exit, the airline gate agent may conduct manual identity verification using the presented travel document, as is performed for flights where biometric processing is not available, and may notify CBP to conduct further examination, if necessary. For example, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship. As previously explained, biometric entry-exit is not a surveillance program. Rather, the entry-exit program will be used to confirm the identity of travelers and verify that they are the authorized bearers of their travel documents. Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure is essential for addressing the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who

¹⁶⁰ See the NPRM, 85 FR at 74164, for more information regarding DHS' statutory authority to require biometrics.

overstay their authorized period of admission (overstays) or are present in the United States without being admitted or paroled, and incorrect or incomplete biographic data for travelers.

Comment: Some commenters raised concerns regarding the Fourth Amendment protection against unreasonable searches and seizures.

Response: Regarding the Fourth Amendment, DHS's biometric entry-exit program complies with the Fourth Amendment and is consistent with the Congressional mandate to enact such a program. *See* section 110(b) of the DMIA (8 U.S.C. 1365a(b)) and section 7208(d) of the IRTPA (8 U.S.C. 1365b(d)). To exercise its authority to control the border and to regulate the entry and departure of both aliens and U.S. citizens, CBP has a legitimate interest in confirming the identity of arriving and departing travelers and verifying that such persons are the authorized bearers of proffered travel documents. *See* INA 215, 235 (8 U.S.C. 1185, 1225). The use of facial comparison technology in DHS's entry-exit program is non-invasive and aligns with the Congressional requirement to develop such a program.

Comment: Some commenters raised concerns regarding the Fifth Amendment due process requirements.

Response: Regarding the Fifth Amendment, the entry-exit program does not deprive an individual of a constitutionally protected liberty interest. Similar to the practice of manual identity verification where biometric processing is not available, facial comparison technology will be utilized for identification purposes. For example, as is currently the practice on exit, during the manual review of the passport, if there is some question as to the authenticity of the passport or whether the person presenting the passport is the person to whom the passport was lawfully issued, airline partners will contact CBP for additional inspection, and a CBP officer may perform a manual review of the passport. A CBP officer may ask questions to validate identity and citizenship.

Requiring the submission of biometrics for identification purposes does not violate the Fifth Amendment's due process requirements nor does collecting and retaining certain biometric information deprive individuals of a liberty interest. DHS requires submission of biometrics as authorized by law.

Comment: One commenter raised concerns regarding the Sixth Amendment right to counsel.

Response: Regarding the Sixth Amendment, this right to counsel would not apply as these travelers have not been placed in criminal proceedings.

Comment: One commenter raised concerns regarding the Fourteenth Amendment right to equal protection.

Response: Regarding the rule giving rise to claims under the Fourteenth Amendment's Equal Protection clause, this rule does not affront the Fourteenth Amendment. DHS does not treat people differently based on any biological or physical characteristic of the affected person and nothing in this rule authorizes officers to do so. As explained previously, nothing in this rule will prevent refugees from receiving protections since, other than requiring biometrics for certain new populations, this rulemaking does not change eligibility requirements for asylum seekers or refugees and does not alter existing regulations at 8 CFR 208.6 protecting the confidentiality of information contained in or pertaining to asylum applications and certain other records, and which are also applied to information contained in refugee applications as a matter of departmental policy.

*o. Authority for Biometric Collection and Related Regulations
for Biometric Collection*

Comment: Several commenters raised concerns regarding DHS's authority to specifically collect a "faceprint" as a biometric identifier as Congress has equated biometric identifiers with fingerprints. A commenter stated that 6 U.S.C. 1118 expressly

disallows the expansion of biometrics collections in immigration. Some commenters stated that the use of facial comparison technology is an overreach of power.

Response: DHS is not exceeding its authority to collect biometrics , including 6 U.S.C. 1118, which states that nothing in this section shall be construed to permit the Commissioner of CBP to “facilitate or expand the deployment of biometric technologies, or otherwise collect, use, or retain biometrics, not authorized by any provision or amendment made by” the IRTPA or the Implementing Recommendations of the 9/11 Commission Act.¹⁶¹

DHS laid out both the general and specific statutory authority for biometric collection, including photographs, in the NPRM, and restates much of that explanation of authority in this final rule, and disagrees with commenters that it does not have authority to promulgate this rulemaking.¹⁶² DHS’s statutory authorities, including INA 287(b) (8 U.S.C. 1357(b)), authorize the collection of biometrics when such information is material or relevant to the furtherance of DHS’s delegated authority to administer and enforce the INA. Establishing and verifying an individual’s identity through the use of biometrics falls within DHS’s authority in the administration and enforcement of immigration laws.

Comment: One commenter said that DHS failed to mention a companion proposal to expand types of biometrics collected by USCIS.

Response: Any proposals by USCIS to expand biometrics is outside the scope of this rulemaking. While the NPRM did reference the USCIS NPRM, as noted above, the USCIS NPRM has now been withdrawn. *See* 86 FR 24750.

¹⁶¹ Sec. 1919(b) of the FAA Reauthorization Act of 2018, Pub. L. 115-254, 132 Stat. 3186, 3559 (6 U.S.C. 1118(b)).

¹⁶² *See* the NPRM, 85 FR at 74164, for more information regarding DHS’ statutory authority to require biometrics.

Comment: Several commenters raised concerns regarding CBP's decision to utilize one to few (1:n) matching instead of one to one (1:1), which CBP has tested and some consider safer from a privacy perspective. Additionally, several commenters indicated that CBP has not sufficiently evaluated alternatives.

Response: CBP respectfully disagrees. As mentioned in the NPRM, CBP considered many types of biometrics and has concluded that partnering with carriers and airports to capture facial images is the most viable large-scale solution as it is highly effective, cost effective, and less disruptive than other possible methods.¹⁶³ Two other methods that were considered were fingerprint and/or iris scans and using CBP personnel and equipment to collect the facial scans. CBP has tested fingerprint and iris scans on a limited basis to determine their effectiveness and scalability. CBP found that although these scans are highly effective in finding matches when data is available, they have numerous problems. First, CBP often lacks data to match against. Although CBP often has fingerprints from entry that it can use to match a departing alien, it does not typically capture iris scans. Additionally, these biometrics are not typically included in passports. To use iris scans, CBP would need to establish a new way to capture a baseline iris scan to compare against at exit, which is not feasible. Fingerprint and iris scans are also more time-consuming and the equipment needed is more expensive than facial comparison.

Although CBP does use 1:1 verification, using strictly 1:1 verification would add a substantial amount of processing time to each inspection, which would negatively affect CBP's mission of facilitating travel. On entry, CBP utilizes 1:1 comparison in the pedestrian environment for travelers that possess an e-chip photo consistent with Western

¹⁶³ See the NPRM, 85 FR at 74169-74173, for more information regarding CBP's tests to determine the best option for biometrics collection.

Hemisphere Travel Initiative (WHTI) requirements. For other travelers, CBP is able to create galleries based on the manifest information received from carriers for air, sea, and bus travelers. The galleries allow for a 1:n comparison, which is faster and less intrusive to the travelers.

On exit, a 1:1 verification would require private sector partners to procure additional equipment that can open and read e-chips, when available, and collect and submit more information to CBP. This is both costly and time-consuming as well as an increase in the privacy implications on the public. As with entry, CBP is able to create galleries based on manifest information received from carriers for air, sea, and bus travelers. The galleries allow for 1:n comparison which is faster and less intrusive to the travelers.

Comment: One commenter suggested an alternative “opt-out” option available to U.S. citizens can be extended to aliens in lieu of additional alternatives.

Response: Upon the effective date of this final rule, all aliens seeking admission to and departing from the United States may be subjected to facial comparison to determine identity or for other lawful purposes. CBP bears the ultimate responsibility for biometric collection to satisfy the Congressional biometric entry-exit mandate. Partner airports and carriers facilitate collection through the use of CBP’s TVS, which provides an automated mechanism to verify identity.

Additionally, as part of the inspection process, DHS is authorized to take and consider evidence (including biometrics) concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of the INA and the administration of DHS. *See* INA 287(b) (8 U.S.C. 1357(b)).

Comment: One commenter asked why DHS intends to collect both fingerprints and facial comparison data.

Response: As discussed in the NPRM and this final rule, fingerprint scans have proven to be an effective law enforcement tool, which is why CBP will continue to capture fingerprints as the initial identification biometric.¹⁶⁴ CBP may elect not to collect fingerprints for subsequent identity verification where CBP has implemented facial comparison.

q. Rule Impact on Migration, Immigration, and National Security

Comment: Several commenters raised concerns that DHS failed to justify collecting facial images from the proposed individuals and that by collecting photographs circular migration is affected, vulnerable populations, including asylum seekers and refugees, are deterred from fleeing persecution, and immigrants are at risk of future violence and losing their immigration status in the name of national security.

Response: DHS disagrees with these comments. As discussed in the NPRM, DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States.¹⁶⁵ CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient. Upon the effective date of this final rule all aliens entering or exiting the United States may be subjected to facial comparison, regardless of age, gender, or race and nationality. This rule will not “extend to everyone associated with an immigration case” as asserted by a commenter.

This rule improves DHS’s ability to meaningfully implement a comprehensive biometric entry-exit system and make the process for verifying the identity of aliens more

¹⁶⁴ See the NPRM, 85 FR at 74173, for more information on fingerprint collection as the initial biometric.

¹⁶⁵ See the NPRM, 85 FR at 74164, for more information regarding DHS’ statutory authority to require biometrics.

efficient, accurate, and secure by using facial comparison technology. Implementing an integrated biometric entry-exit system that compares biometric data of aliens collected upon arrival with biometric data collected upon departure is essential for addressing the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who overstay their authorized period of admission (overstays) or are present in the United States without being admitted or paroled, and incorrect or incomplete biographic data for travelers.

In this final rule, DHS thoroughly discusses how facial comparison mitigates the above-mentioned national security concerns. Nevertheless, the totality of the screening system must be taken into account when discerning the national security benefits. As discussed in the 9/11 Commission Report, biometric entry-exit is essential to national security and should include a systemic approach that balances security, efficiency and civil liberties.¹⁶⁶

CBP's responsibilities, regardless of age, gender, race and nationality, include ensuring the interdiction of persons illegally entering or exiting the United States, facilitating and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States. *See* sec. 411(c) of the Homeland Security Act (6 U.S.C. 211(c)). CBP uses the totality of information available, to include the results of a facial comparison match, to fulfill these responsibilities.

Biometric entry-exit is an identity verification tool. As previously explained, the biometric entry-exit program uses facial comparison technology to ensure a person is

¹⁶⁶ The 9/11 Commission Report 385-386 (2004) (emphasis added), available at <https://9-11commission.gov/report/> (last visited May 21, 2025).

whom the person says the person is – the bearer of the passport the person presents.

Biometric entry-exit is complementary to CBP’s multilayered enforcement approach and border security mission.

DHS has no data or evidence, and the commenters provide only assertions and not any empirical evidence, studies, or reports, to support the statement that photograph submission reduces circular migration, deters vulnerable populations from fleeing persecution or causes a decline in U.S. tourism or the U.S. economy. DHS’s intent for this rule is explained in detail herein.

Nothing in this rule prevents refugees from receiving protections since, other than requiring biometrics for certain new populations, this rulemaking does not change eligibility requirements for asylum seekers or refugees and does not alter existing regulations at 8 CFR 208.6 protecting the confidentiality of information contained in or pertaining to asylum applications and certain other records, and which are also applied to information contained in refugee applications as a matter of departmental policy.

Comment: One commenter discouraged DHS/CBP from seeking to justify this NPRM by securing TSA’s adoption of facial biometric comparison using TVS in domestic airports.

Response: In the cost-benefit analysis, DHS noted in the NPRM that the development of a reliable facial comparison system could also have benefits for the U.S. government as a whole, including TSA.¹⁶⁷ This is not a justification for the rule, but rather a secondary benefit. Furthermore, DHS strives to build a more unified and operationally effective and efficient organization through collaboration across DHS. TSA has leveraged TVS for baggage drop and TSA check points, which increases DHS’s operational effectiveness by reducing unnecessary duplication and redundancy. As with

¹⁶⁷ See the NPRM, 85 FR at 74188, for more information on the benefits to the U.S. government.

the current CBP-TSA uses of TVS, any future use of TVS, whether for international or domestic travelers, will undergo all necessary legal and privacy assessments and evaluations.

Comment: Some commenters stated that taking a photo will add more burden, confusion, and harassment at the ports of entry.

Response: CBP respectfully disagrees as nothing in the rule is meant to burden, confuse, intimidate, or harass aliens at the ports of entry. As mentioned in Section III.B.1 above, CBP has determined that facial comparison technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient. It relies on current traveler behaviors and expectations; most travelers are familiar with cameras and do not need to learn how to have a photograph taken, minimizing any confusion. Should travelers express any confusion either a CBP officer or a gate agent can guide them through the new process or provide a tear sheet with additional information.

Furthermore, each CBP employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws, and ethical principles above private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the Code of Federal Regulations. *See* 5 CFR part 2635. Additionally, Section 7.11.2 of the CBP Standards of Conduct specifically states, “Employees will not make abusive, derisive, profane, or harassing statements or gestures, or engage in any other conduct evidencing hatred or invidious prejudice to or about another person or group on account of race, color, religion, national origin, sex, sexual orientation, age, or disability.” CBP Directive 51735-013B, Standards of Conduct at 11 (2020), available at https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf (last visited May 15, 2025).

Comment: Several commenters noted that per CBP’s FY 2020 Trade and Travel Report, no imposters were identified in the air environment during FY2020.

Response: CBP expanded the number of locations with facial comparison technology and as a result biometrically processed more travelers compared to FY2019; however, as noted in the Trade and Travel Report, CBP saw a decrease in traveler volume of 42 percent in FY 2020 when compared to data from FY 2019, which may have affected the number of imposters identified. Nevertheless, as traveler volume has increased CBP has seen an increase in the number of imposters identified with 2,000 imposters identified at land ports and airports.¹⁶⁸

Comment: One commenter noted that CBP is attempting to move the goal posts it had originally established for the use of facial comparison technology in airports from national security to pandemic mitigation.

Response: Although CBP’s primary responsibility is national security, CBP must also facilitate legitimate trade and travel. The use of facial comparison technology, as explained in this final rule, has enabled CBP to not only address a national security concern head-on by enhancing identity verification but to simultaneously improve the traveler experience throughout the travel continuum. This is not an attempt “to move the goal posts,” but rather an opportunity to showcase the several benefits that facial comparison technology provides. As CBP continues to use the technology and threats evolve, additional benefits are identified, such as the use of biometrics to mitigate the transmission of pathogens. As noted by the commenter, CBP may take other steps to mitigate the transmission of pathogens, such as installing plexiglass at the primary

¹⁶⁸ See CBP, Biometrics, <https://www.cbp.gov/travel/biometrics> (last modified Oct. 5, 2023) (last visited May 21, 2025).

inspection booths; however, implementing one mitigation measure does not reduce the need for additional measures, especially when dealing with a global health crisis.

r. Proposed Amendments to the Regulations

Comment: Several commenters raised concerns regarding the proposed addition of “or other lawful purposes” in 8 CFR 215.8 (a)(1) and 8 CFR 235.1(f)(1)(ii) as they asserted the language is vague and would expand the use of photographs captured upon the entry into or the exit out of the United States beyond what is authorized in regulations as they existed prior to this final rule.

Response: DHS disagrees with these comments. As discussed in the NPRM, DHS is mandated by statute to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States.¹⁶⁹ As articulated in section 7208 of the IRTPA (8 U.S.C. 1365b), the biometric entry-exit system serves several purposes; this includes recording entries and exits of aliens to the United States. The entry-exit system may also be used to determine whether an alien has properly maintained immigration status while in the United States. Once collected, and to the extent the data is maintained for any length of time, the information may be used to support other lawful enforcement purposes. Section 7208 of the IRTPA (8 U.S.C. 1365b) does not limit CBP’s use of the data to simply the entry-exit purpose.¹⁷⁰ In addition, as previously explained, the biometric entry-exit does support CBP’s border security mission and is complementary to the agency’s multilayered enforcement approach.

As stated in 8 CFR 215.8(b) prior to the effective date of this final rule, “an alien who is required to provide biometric identifiers at departure...who fails to comply with

¹⁶⁹ See the NPRM, 85 FR at 74164, for more information regarding DHS’ statutory authority to require biometrics

¹⁷⁰ See TVS PIA at 16-17 for more information on the permissible uses of this data.

the departure requirements may be found in violation of the terms of his or her admission, parole or admission status.” DHS is simply expanding the scope of aliens that are subject to that requirement.

Comment: Additionally, commenters raised concerns about requiring certain aliens entering and departing the United States to “provide other biometrics” and “other such evidence requested,” which is overly broad and ambiguous.

Response: DHS has the authority under both 8 CFR 215.8 and 235.1 to request that aliens provide biometrics and “such other evidence as may be requested.” DHS is not expanding its authority by continuing to request other evidence.

Comment: One commenter opined that DHS proposes to coerce immigrants to provide an unjustified amount of private information under the threat of losing their immigration status.

Response: DHS disagrees with this comment. DHS requires submission of biometrics as authorized by law. Additionally, DHS is mandated to implement a biometric entry-exit system.

Comment: Some commenters raised concerns that the definition of “biometrics” was being expanded to include DNA, iris scans, and palm prints.

Response: As discussed in this final rule, to continue to allow flexibility for DHS to employ different methods of biometric collection in the future, DHS is amending 8 CFR 215.8(a) and 235.1(f) to provide that any alien, other than those exempt by regulation, may be required “to provide other biometrics” upon arrival into and departure from the United States. CBP has tested iris technology, for example, but biometric technology continues to advance and there may be other biometric options that may have potential for implementation in the future. Additionally, any collection of any biometrics will be consistent with U.S. law.

s. *Land and Sea Implementation*

Comment: Some commenters requested that CBP suspend the proposed rule change until such time that a biometric exit solution for land and sea ports is identified. In the absence of a tested and compatible solution at land and sea ports, it is not appropriate for CBP to forge ahead across all airports and cement a collection and matching program that it may not be possible to operationalize at land and sea ports. One commenter indicated that further details on process, timing, cost, etc., in the land and sea environments are necessary to ensure traveler confidence and comprehension.

Response: The regulatory changes are necessary to enable CBP to continue its refinements and implement permanent programs efficiently once the best solution is identified. Under the regulations prior to the effective date of this final rule, CBP could conduct pilot programs only at a limited number of ports of entry at air and sea and could collect biometrics only from a limited population. Pursuant to this final rule, CBP will continue to work to determine the best method for implementation as necessary. In the time since the NPRM was published, CBP has implemented facial biometric collection fully at air entry, sea entry, and pedestrian land entry. Further details about those environments can be found in Section VI of this rule. Additionally, when CBP moves forward with a large-scale implementation for entry-exit at land ports or for private aircraft or for exit at sea ports, CBP will publish a notice in the *Federal Register* providing information regarding details of implementation in each new environment and requesting comments on the newly implemented transportation modalities. If CBP determines that the implementation of the specified facial comparison entry-exit program at land ports or exit at sea ports results in significant delays, CBP will temporarily discontinue these efforts until the average processing time has improved to be under 125 percent of the baseline (manual processing without biometrics).

t. Implementation Challenges

Comment: Some commenters said this rule does not mention any implementation challenges that have been encountered with the currently deployed biometric system, which directly affects CBP's ability to achieve the benefits outlined in this rule. CBP should develop photo capture requirements and camera system standards and requirements for at least three consecutive months to reduce malfunction and successfully capture each traveler.

Response: CBP disagrees with the premise of these comments. As discussed in the NPRM and in this final rule, CBP is using biometric technologies in partnership with commercial stakeholders.¹⁷¹ In order to use CBP's TVS, partners must meet all of CBP's business and technical requirements, such as internet/connection guidelines, photo specifications and equipment parameters. It is important to note that, unlike FIS areas, the airport departure areas are not managed by CBP personnel; however, CBP works closely with the stakeholders to mitigate any issues that may affect system performance. CBP has a suite of tools that allows for system and operational performance management and CBP uses performance reports that are automatically generated and distributed weekly within CBP and to external stakeholders. CBP monitors the reports for performance issues and addresses any anomalies with stakeholders as they arise. The reports are also used to promote/increase usage by stakeholders.

u. Cost and Cost-Benefit Analysis Concerns

Comment: Some commenters raised concerns surrounding the costs associated with this rule. One comment stated that this is a waste of government resources. One commenter indicated that the money used for this program should be redirected to more deserving programs such as uniting children. Another suggested the money should be

¹⁷¹ See the NPRM, 85 FR at 74178, for more information on business partnership requirements.

spent rooting out corruption, incompetence, extremism, and politics from our law enforcement agencies and armed forces.

Response: Allocation of money for agencies is determined by Congress as part of its appropriation process. It is not within DHS's authority to reallocate money appropriated by Congress for a specific purpose to a different purpose. In FY 2016, Congress authorized the funding of the original, biometric entry-exit program through up to \$1B in fees, collected by USCIS, on H-1B/L-1 applications, through FY 2027.¹⁷²

Further, DHS is statutorily mandated to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Additionally, DHS believes that the purposes of this rule, namely to deploy a comprehensive biometric entry-exit system and enable CBP to make the process for verifying the identity of aliens more efficient, accurate, and secure by using facial comparison technology, as well as the national security and immigration benefits—such as helping detect and deter visa overstays and visa fraud; helping identify persons attempting to fraudulently use travel documents; and alerting authorities to criminals or known or suspected terrorists prior to boarding—are all appropriate uses of DHS and the administration's time and resources. DHS disagrees strongly that this rule is a waste of taxpayer funds.

Comment: A few commenters suggested that the analysis did not present all the costs associated with this rule, and that the actual costs would be significantly higher than CBP's estimate, suggesting that there was not sufficient data presented in the cost-benefit analysis to support this rule. Additionally, the rule allows for expansion of biometric collection at sea and land port locations but such costs are not provided in the analysis,

¹⁷² See Consolidated Appropriations Act, 2016, Div. O, sec. 402(g), Pub. L. 114-113, 129 Stat. 2242, 3006, as amended by sec. 30203(b) of the Bipartisan Budget Act of 2018, Pub. L. 115-123, 132 Stat. 64, 126.

therefore CBP is proposing to be given such authority regardless of the data collection method or costs.

Response: DHS disagrees that there was not sufficient data presented in the cost-benefit analysis to support this rule. As explained in the rule, CBP is using biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders. Based on agreements with CBP, these stakeholders deploy their own camera operators and camera technology to operate TVS for identity verification. CBP expects that the use of facial comparison to collect biometric information will help streamline the entry and exit process, generating efficiencies to CBP, carriers, and travelers. Additionally, it will support CBP's capability in determining whether aliens are departing the country when they are required to depart, reduce visa, or travel document fraud, and improve CBP's ability to identify criminals and known or suspected terrorists before they depart the United States. In recent years CBP has implemented a variety of pilot programs to test the collection of this biometric information during entry and exit. Therefore, CBP does have some past data available to provide an estimate of overall costs and benefits during the pilot test program period. CBP expects that the data obtained during the pilot period assists in generating a reliable estimate of future costs and benefits from collection of this biometric information.

The analysis for the NPRM was done using the standards required under Executive Order 12866 and 13563 and is in compliance with the Regulatory Flexibility Act. Specific guidance on how agencies should conduct cost benefit analyses for regulations can be found in OMB Circular A-4. Regulatory analysis should monetize any effects that can be monetized. Those that cannot be monetized should be analyzed quantitatively, if possible. Those that cannot be monetized or quantified should be analyzed qualitatively. The analysis for the NPRM was done based on the best information available at the time. When the NPRM had been written, biometrics had not

yet been deployed in all environments, so it was impossible to conduct a quantitative analysis for those environments. For this final rule, CBP has updated the estimates in the NPRM and has expanded it to include several new use-cases. There are still environments where CBP has not implemented a biometric process. For these environments lack of information and details make it impossible to monetize or quantify the effects, so CBP provides qualitative discussion based on limited details that were available at the time of the final rule on future biometric process implementation provides qualitative so we analyze them qualitatively.

DHS acknowledges that there will be costs associated with this final rule. DHS has updated the regulatory impact analysis for this final rule to reflect more recent data and information to improve DHS's best estimate of this rule's costs and benefits, including the expansion of facial comparison biometric collection to additional environments beyond the air environment. According to the regulatory impact analysis for this rule, DHS determined a net cost of \$572 million (in undiscounted 2024 U.S. dollars) during the pilot period (2017–2024) and estimates a net cost of \$287 million (in undiscounted 2024 U.S. dollars) in the 5-year regulatory period 2025–2029.

Because CBP has not determined the best approach to implement biometric collection at entry-exit for private aircraft, at exit at land ports, at entry for travelers in vehicles or for exit at sea ports, CBP is unable to provide any estimates for these costs to implement a biometric entry-exit system nationwide to these environments. This rule provides CBP authority to establish biometric entry-exit on a nationwide basis but CBP acknowledges that due to lack of information at this time, when CBP moves forward with a large-scale implementation for entry-exit biometric collection for private aircraft, at exit at land ports, at entry at land ports for travelers in vehicles or for exit at sea ports, CBP will publish a notice in the *Federal Register* with information regarding details of implementation and request comments on the newly implemented transportation

modalities. DHS asserts that the regulatory impact analysis for this final rule is sufficient to meet DHS's obligations under Executive Orders 12866, 13563, and 14192.

Comment: A few commenters were concerned with the voluntary opt-out rate of U.S. citizens used in the regulatory impact analysis, specifically commenters believe that the opt-out rate used in the economic analysis for this rule significantly underestimated the number of U.S. citizens that would opt-out of having their photographs taken for use of facial comparison during biometric collection.

Response: CBP originally determined the U.S. citizen opt-out rate to voluntarily participate in the biometric exit program was 0.18% and was based on a 2-day sample in 2019 of 13,000 travelers at a single airport location.¹⁷³ CBP conducted a time and motion study to verify and reassess the 0.18% opt-out rate in late August 2021.¹⁷⁴ From this CBP Time and Motion Study CBP determined that the opt-out rate for biometric exit collection in the air environment was approximately 0.28% of outbound travelers. CBP uses this new estimate in the regulatory impact analysis for the final rule, to calculate future U.S. citizens who will opt-out of facial comparison during biometric collection at exit in the air environment.

To determine the opt-out rate for U.S. citizens during facial comparison at Simplified Arrival for biometric collection at entry, CBP used data from internal databases to calculate the actual number of opt-outs compared to the total number of U.S. citizen inbound air travelers processed through Simplified Arrival. CBP calculated the opt-out rate for U.S. citizens at entry during biometric collection through Simplified Arrival was approximately 0.13%. CBP used this estimate to calculate the number of

¹⁷³ See the NPRM, 85 FR at 74183, regarding the opt out rate estimate at the time of NPRM publication.

¹⁷⁴ CBP, Biometric Air Exit Time and Motion Study (2021) (CBP Time and Motion Study). This internal study was conducted August 22 through September 1, 2021, and is discussed in greater detail in the full regulatory impact analysis of this final rule in a separate document included in the docket for this rulemaking, docket number [USCBP-2020-0062].

U.S. citizens who will opt-out of facial comparison at entry during Simplified Arrival during the regulatory period of the regulatory impact analysis for the final rule. CBP also used this opt-out rate of approximately 0.13% to estimate the number of U.S. citizens who will elect to opt out of facial comparison biometric collection during entry processing at Simplified Arrival in the sea environment and at Mobile Face Primary in the sea environment.

To account for U.S. citizens opting out of facial comparison biometric collection at entry in the sea environment during Facial Biometric Debarkation, CBP used the same opt-out rate that was determined from the CBP Time and Motion Study for travel industry-led facial comparison biometric collection in the air environment of approximately 0.28% discussed above. Additionally for pedestrians entering the United States in the land environment and who are processed through Pedestrian Entry, CBP used internal data to determine that approximately 0.21% of U.S. citizens elected to opt out of facial comparison biometric collection. CBP used this rate to estimate the number of U.S. citizen pedestrians that would elect to opt out of facial comparison biometric collection when processed through Pedestrian Entry, in the regulatory impact analysis for this final rule.

Comment: One commenter argued that a Regulatory Flexibility Analysis (RFA) should have been conducted pursuant to the Regulatory Flexibility Act as individuals could potentially be small businesses, including sole proprietors, self-employed individuals, and freelancers, representing small entities, therefore a significant number of small entities could be affected, and this rule warrants a complete RFA.

Response: DHS does not believe an RFA was required for the NPRM. The Regulatory Flexibility Act (5 U.S.C. 601 *et. seq.*), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104-121, 110 Stat. 857), requires agencies to consider the impacts of their rules on small entities. This final rule directly

regulates individual travelers, which are not small entities. However, CBP does not anticipate that this rule will result in any significant impact to individual travelers, as according to the analysis individual travelers will likely incur an insignificant time burden during exit and time savings during entry.

Comment: A few commenters were also concerned with CBP's proposed timeline for implementation of the biometric exit program (97% implemented by 2024), specifically as the air industry had been hurt significantly in 2020.

Response: CBP has still not yet reached 97% implementation, but is continuing to work with carriers and airports to establish partnerships to implement this program nationwide. These partnerships with carriers and airports streamline the process and eliminate redundancies. As explained in detail in the robust economic analysis, the hardware cost will be borne by the carriers and airports who partner with CBP. CBP will give carriers and airports access to its facial comparison system and the carriers and airports will choose (and pay for) the hardware that best fits their needs. Despite disruptions to the airline travel industry from the COVID-19 pandemic and negative economic impacts, there continues to be significant interest from the airline industry to use facial comparison. CBP continues to work to fully implement biometric collection at air exit as soon as possible. This Public-Private Partnership aligns with CBP's Resource Optimization Strategy.¹⁷⁵

Comment: Additionally, a few commenters were concerned with the lack of discussion regarding costs to individuals that could result in potential delays resulting from a no match situation during boarding.

¹⁷⁵ See CBP, Resource Optimization Strategy, <https://www.cbp.gov/border-security/ports-entry/resource-opt-strategy> (last visited May 21, 2023).

Response: CBP does not expect there to be any delays as a result of no match situations during the boarding process on flights where biometrics are being collected. In the event of a no match during facial comparison, the airline staff will manually observe the individual's travel documents using the same process that takes place absent this rule. Additionally, CBP does not anticipate that in the event of a no match, that a CBP officer would be asked to verify an individual's travel documents more frequently than what occurs prior to the implementation of this rule.

VI. Request for Comment

As discussed above, DHS is issuing a final rule to finalize the changes proposed in the NPRM. However, DHS is requesting comments regarding the specific method of collection for newly implemented transportation modalities as well as costs and benefits for the newly implemented transportation modalities, namely, the Simplified Arrival process at air entry, the sea entry processes, and the process for entry for pedestrians at land ports. Comments submitted regarding any other topic on these newly implemented transportation modalities are out of scope for this final rule and will not be considered

DHS will also provide notice and seek comments for future implementations of facial biometric collection in line with the authorities discussed in this rule.

VII. Statutory and Regulatory Requirements

A. Executive Orders 12866, 13563, and 14192

Executive Orders 12866 (Regulatory Planning and Review) and 13563 (Improving Regulation and Regulatory Review) direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. Executive Order 14192 (Unleashing Prosperity

Through Deregulation) directs agencies to significantly reduce the private expenditures required to comply with Federal regulations and provides that “any new incremental costs associated with new regulations shall, to the extent permitted by law, be offset by the elimination of existing costs associated with at least 10 prior regulations.”

This rule has been designated a “significant regulatory action” that is economically significant, under section 3(f)(1) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget.

Pursuant to section 5(a) of Executive Order 14192, the requirements of that Executive Order do not apply to regulations issued with respect to a national security or homeland security function. As discussed in this preamble, the primary, direct benefit of this rule is improvement in national and homeland security. Accordingly, this rule is exempt from the requirements of Executive Order 14192.

In summary, during the period of analysis, FY 2017–2029, CBP expects there to be costs, and benefits from this final rule, resulting in annualized net costs ranging from \$67.9 million in 2024 U.S. dollars (using a three percent discount rate) to \$70.3 million in 2024 U.S. dollars (using a seven percent discount rate) to the Federal Government, the air travel industry, the sea travel industry and alien and U.S citizen air travelers, sea travelers and land pedestrian travelers. The final rule will result in the non-monetized benefit of improving national security by validating the identity of individuals entering and exiting the United States. CBP expects this final rule will improve CBP’s ability to detect and deter visa overstays and visa fraud, identify persons using fraudulent travel documents and the detection of criminals or known or suspected terrorists at entry or exit. The following is an abbreviated analysis of the costs, cost savings and benefits of this final rule. The full regulatory impact analysis of this final rule is in a separate document included in the docket for this rulemaking, docket number [USCBP-2020-0062].

DHS is statutorily mandated to develop and implement an integrated, automated entry and exit data system to match records, including biographic data and biometrics, of aliens entering and departing the United States. Since 2004, DHS, through CBP, has been collecting biometric data from aliens arriving in the United States, but currently there is no comprehensive biometric system in place to track when the aliens depart the country. Since taking over management of biometric entry and exit operations in 2013, CBP has been testing various options to collect biometrics at arrival and departure. The results of these tests and the recent advancement of facial comparison technology have provided CBP with a model for moving forward with implementing a comprehensive biometric exit solution in the air environment as well as improving the collection of biometrics at entry in the air, sea, and land environments.

CBP has developed a process for using facial comparison technology to collect biometrics in the commercial air environment, at entry in the sea environment and at entry for pedestrians in the land environment; however, CBP is still determining the best approach to expand the collection of biometrics using facial comparison technology for processing travelers in vehicles entering the United States in the land environment or a comprehensive solution for travelers at exit in the sea and land environments. CBP continues its work to determine the best option for biometric collection in these environments. At this time CBP has implemented comprehensive facial comparison biometrics at entry in the air, sea, and land (pedestrians only) environments and at exit only in the air environment.

During the initial stage of implementation for biometric collection at exit in the commercial air environment, starting in 2016, CBP introduced facial comparison technology to a limited number of airports in a voluntary pilot program. These deployments allowed CBP to fine-tune the process of using facial comparison technology for biometric collection at exit, while also partnering with airline carriers and airports (the

air travel industry) toward a nationwide implementation. CBP's biometric exit program in the air environment was initially limited to 15 locations during the pilot period. CBP has since partnered with air travel industry members voluntarily expanding the program to additional locations. CBP has been able to find willing partners from the air travel industry as the industry has recognized the benefits of streamlining the boarding process and creating a seamless touchless experience for air travelers using facial comparison technology throughout the entire airport, from verifying identity, to obtaining boarding passes, checking bags, passing security and boarding. Additionally, the touchless passage through an airport may mitigate the risk of pathogen transmission.¹⁷⁶

The facial comparison system engineered and developed for biometric exit in the air environment, known as the Traveler Verification Service (TVS) has also been implemented in other environments. CBP used the TVS when developing a program to use facial comparison technology to collect biometrics at entry in the commercial air environment, known as the Simplified Arrival process (Simplified Arrival), expediting the entry process for inbound air travelers, and improving security measures. Prior to Simplified Arrival, most inbound alien air travelers were already photographed during the entry process into the United States. Simplified Arrival compares the photographs collected at arrival to the passport, which expedites the arrival process. Because the infrastructure was already in place to take photographs of aliens, CBP was able to complete the entire nationwide deployment of Simplified Arrival in the air environment by the end of 2022. The entry processes in the air and sea environments are similar and in certain locations CBP was able to introduce Simplified Arrival in the sea environment starting in 2021 to use facial comparison technology for biometric collection of some

¹⁷⁶ Information provided by CBP's Innovation and Strategy Directorate, Biometrics Program Office, Office of Field Operations, subject matter expert on March 18, 2022.

inbound sea travelers.¹⁷⁷ By the end of 2023, CBP had fully implemented Simplified Arrival in the sea environment with operations at 39 sea port locations where the entry process in the sea environment was similar to entry in the air environment.

Where the entry process differs between the air and sea environments and Simplified Arrival was not a viable option, TVS allowed CBP to implement additional processes for biometric collection using facial comparison technology at entry. Starting in 2018, CBP began working with the sea travel industry to introduce facial comparison biometric collection at entry in the sea environment for certain sea travelers. Sea travel industry members voluntarily participated in conducting FBD, which uses facial comparison technology hardware procured by the sea travel industry in coordination with CBP's TVS to confirm passenger identity at entry.¹⁷⁸ CBP also implemented another biometric collection process using TVS for facial comparison at entry in the sea environment known as Mobile Primary Face. When cargo vessels arrive at a U.S. sea port, CBP officers typically conduct entry processing of crew members onboard the cargo vessel. The introduction of Mobile Primary Face allowed CBP officers with mobile devices to conduct biometric collection using facial comparison technology for cargo vessel crew members. The implementation of these biometric collection processes at entry in the sea environment using facial comparison technology has expedited the arrival process for many inbound sea travelers.

CBP was also able to use TVS and the Simplified Arrival process to develop a biometric collection process using facial comparison technology during the entry process

¹⁷⁷ CBP implemented a few different biometric collection processes at entry in the sea environment because of different treatment of sea travelers prior to the implementation of biometric collection using facial comparison technology. Simplified Arrival was implemented at 39 sea ports to process certain cruise vessel passengers and most cruise vessel crew members.

¹⁷⁸ FBD was implemented by sea travel industry members for only certain types of cruise vessel arrivals. The entry process for a cruise is different depending on if the cruise is classified as an open or closed loop cruise. FBD is conducted only for entry processing of closed loop cruise passengers who have passports.

for pedestrians in the land environment, known as Pedestrian Entry. The entry process for pedestrians in the land environment is similar to other environments such that travelers go through a CBP inspection where they provide their travel documents (e.g., passport) and the CBP officer manually inspects the documents to verify the identity of the traveler and determine admissibility. During this entry process most inbound alien pedestrian travelers are photographed and often have their fingerprints taken to verify their identity. Pedestrian Entry allows CBP to use facial comparison technology instead of conducting manual inspections of travel documents and obtaining fingerprints, resulting in an expedited entry process for pedestrians in the land environment. Similar to entry in the commercial air environment, the infrastructure was largely already in place for CBP to quickly implement Pedestrian Entry. CBP introduced Pedestrian Entry to one pilot location in 2018 and by the end of 2022 Pedestrian Entry had been fully implemented by CBP at 185 locations on the northern and southern border of the United States that process inbound pedestrians.¹⁷⁹

This final rule will allow for the collection of facial biometrics of all aliens at entry and exit. Prior to the effective date of this final rule, most aliens were already subject to photograph at entry; however, some aliens, such as aliens who are under the age of 14 or over the age of 79, were exempt and not required to be photographed at entry or exit. This final rule provides that all aliens, including those previously exempt, may be photographed at entry and exit. U.S. citizens may be photographed at entry and exit under this final rule if they voluntarily participate in biometric collection but retain their ability to opt out of being photographed for the purpose of identity verification using biometric facial comparison. Removing the exemptions for aliens for photographs at

¹⁷⁹ Data provided by CBP's Innovation and Strategy Directorate, Biometrics Program Office, Office of Field Operations, subject matter expert February 18, 2025. CBP implemented Pedestrian entry at all 185 crossings/sites across all 113 land ports of entry.

entry and exit will allow CBP to further expand the facial comparison technology used for the collection of biometrics and provide for a more complete evaluation as CBP moves toward nationwide expansion. Additionally, this final rule will remove the reference in regulations to pilot programs, eliminate the 15-location pilot program air and sea port limit for conducting biometric collection at exit in the air and sea environments, and include authority for CBP to continue the expansion of biometric collection at exit in the sea and land environments and at entry in the land environment.¹⁸⁰

Because CBP is still determining the best option for implementing biometric collection at exit in the sea, land, and private aircraft environments or at entry in the land environment for travelers entering in vehicles or private aircraft, the analysis for this final rule will only discuss the costs and benefits of biometric programs that have been established in the air, sea, and land environments. Capturing images using facial comparison technology during biometric collection at entry and exit as a result of this final rule will affect CBP, air travelers, sea travelers, pedestrian land travelers, the air travel industry, and the sea travel industry. The implementation of the facial comparison technology will also improve CBP's security efforts; provide CBP with greater accuracy in determining whether aliens are departing the country when they are required to depart; reduce visa or travel document fraud; and improve CBP's ability to identify criminals and known or suspected terrorists before they enter or depart the United States.

In the analysis for the final rule, CBP considers the effects from the implementation of facial comparison technology used for biometric collection at exit and entry in the commercial air environment and at entry in the sea environment and at entry

¹⁸⁰ CBP acknowledges that although this final rule grants authority to CBP to expand biometric collection in these environments, CBP does not have a feasible solution to implement such programs at this time. Additionally, when moving forward with additional large-scale implementation of facial comparison technology for biometric collection at land or sea ports, CBP will publish a notice in the *Federal Register* with information regarding details of implementation and request comments on the newly implemented transportation modalities.

for pedestrians in the land environment during the 8-year pilot period spanning fiscal years 2017–2024 and the 5-year regulatory period spanning fiscal years 2025–2029. In addition, CBP provides the total costs, cost savings and net costs during both the pilot and regulatory periods to reflect the total cost of these biometric programs as a whole from 2017-2029. CBP has revised the cost and benefit estimates provided in the analysis for the NPRM in response to public comments to include recently available information and data, including costs and benefits attributable to the implementation of Simplified Arrival, FBD, Mobile Primary Face, Pedestrian Entry, and to include the results from the CBP Biometric Air Exit Time and Motion Study (CBP Time and Motion Study).

In this analysis, CBP analyzes the effect of the biometrics program over two time periods: the pilot period and the regulatory period. In the analysis of the pilot period for the NPRM, CBP only identified costs to CBP and outbound air travelers. CBP had expected that during the pilot period, CBP would be solely responsible for the implementation of biometric exit pilot programs, bearing the costs for installing hardware, and staffing biometric exit collection operations. However, the pilot period has lasted long enough that the air travel industry has voluntarily installed facial comparison technology hardware for biometric collection at exit sooner than CBP had anticipated, allowing CBP to provide estimated costs to the air travel industry during the pilot period in the analysis for the final rule. CBP has also added an analysis of the estimated costs and benefits from implementing facial comparison technology in Simplified Arrival in both the air and sea environments, FBD and Mobile Primary Face at entry in the sea environment, and Pedestrian Entry in the land environment during the pilot period in the analysis for the final rule.

CBP, air travelers, pedestrian land travelers, the air travel industry, and the sea travel industry all experienced costs during the pilot period. Costs during the pilot period to CBP included costs to engineer and develop TVS, procure hardware, provide

management, operation, support, training, and staffing for the implementation of facial comparison technology at entry and exit in the air environment and at entry in the sea environment. Outbound air travelers affected by the biometric exit pilot program incurred time burden costs when boarding flights conducting biometric exit collection, resulting in slightly longer boarding times per traveler. Inbound pedestrian travelers experienced on average slightly longer processing times as a result of being processed through Pedestrian Entry.¹⁸¹ The air travel industry voluntarily incurred costs to procure and install their own facial comparison hardware at departure gates to begin conducting biometric collection at exit, time burden costs from longer boarding times per flight causing additional staffing hours, and costs related to training staff, while conducting biometric operations at departure gates. The sea travel industry also incurred costs to procure and install the necessary hardware required to conduct FBD operations at entry in the sea environment and costs related to training staff to conduct FBD operations. CBP estimated that these costs, shown in Table 2, totaled approximately \$832 million in undiscounted 2024 U.S. dollars over the course of the pilot period, or on average around \$104 million annually.

Cost savings from the implementation of facial comparison technology for biometric collection during the pilot period were experienced by CBP, inbound air travelers processed through Simplified Arrival, inbound sea travelers when processed through Simplified Arrival, FBD or Mobile Primary Face, and sea travel industry members from a swifter debarkation process during FBD. CBP estimates that the cost savings to CBP, inbound air travelers, sea travelers, and the sea travel industry were due

¹⁸¹ CBP notes that the implementation of Pedestrian Entry made the overall entry process in the land environment more efficient. Because of these efficiencies CBP was able to implement changes to the entry process (adding certain functionality and introducing different procedures that the CBP officers have now implemented during the primary inspection process). CBP was unable to separate the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times which CBP estimates resulted in a slightly longer processing time for inbound pedestrian travelers.

to reduced time burdens per traveler as a result of shorter processing times from the use of facial comparison technology at entry. CBP also estimates that the sea travel industry experienced time savings of approximately 1.25 hours per vessel arrival that conducts FBD operations. CBP does not have information available to monetize these time savings but expects the value of these time savings to be significant to sea travel industry members that operate in a very time sensitive business, specifically, when a cruise vessel arrives at a sea port and has to debark passengers, and quickly clean and prepare the vessel for new onboarding passengers and a swift departure. CBP estimated that the total cost savings during the pilot period were approximately \$260 million in undiscounted 2024 U.S. dollars, or on average around \$15.5 million annually. As shown in Table 2, total net costs from this final rule during the pilot period are estimated to be approximately \$572 million in undiscounted 2024 U.S. dollars, or on average \$83.8 million annually.¹⁸²

¹⁸² Net costs during the pilot period could be less than CBP presents here if the actual time burden to the average outbound air traveler and pedestrian traveler is less than CBP estimates or if it actually results in a time savings. CBP notes that actual costs to air travelers from biometric collection at exit when boarding non-CBP biometric flights and for inbound pedestrian travelers processed through Pedestrian Entry are uncertain. The time burden when boarding non-CBP biometric flights could be less than estimated as COVID-19 restrictions eased, and as boarding agents and travelers became more familiar with the facial comparison technology. At entry in the land environment CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times.

Table 2. Pilot Period Net Costs, 2017–2024 (undiscounted thousands of 2024 U.S. dollars)

Fiscal Year	Costs	Cost savings	Net Costs
2017	\$91,818	\$0	\$91,818
2018	\$101,138	\$3,032	\$98,106
2019	\$124,484	\$12,770	\$111,714
2020	\$88,828	\$8,437	\$80,391
2021	\$73,592	\$18,019	\$55,573
2022	\$115,981	\$50,846	\$65,135
2023	\$117,240	\$77,355	\$39,885
2024	\$119,480	\$89,597	\$29,883
Total	\$832,562	\$260,057	\$572,505

Note: totals may not sum due to rounding.

CBP also estimated the effects of implementing facial comparison technology for biometric collection at exit and entry in the commercial air environment and at entry in the sea and land (pedestrians only) environments during the regulatory period. CBP’s analysis for the NPRM did not include costs and benefits from the implementation of the Simplified Arrival process, FBD, Mobile Primary Face, or Pedestrian Entry due to lack of data and information available. In this analysis for the final rule, CBP was able to include these costs and benefits from implementing these biometric collection operations using facial comparison technology and the availability of additional data led CBP to revise its estimated costs and benefits for this final rule during the regulatory period.

CBP, outbound air travelers, inbound pedestrians, the air travel industry, and the sea travel industry will experience costs due to this final rule during the regulatory period. During the regulatory period, CBP expects additional costs to CBP will largely consist of the ongoing maintenance and support activities associated with operating TVS. CBP also anticipates that outbound air travelers will incur a minor time burden per traveler when boarding flights conducting facial comparison for biometric collection at

exit.¹⁸³ CBP expects that inbound pedestrian travelers on average will experience slightly longer entry processing times when processed through Pedestrian Entry, generating an added time burden as a result of this final rule.¹⁸⁴ The air travel industry will also continue to incur hardware procurement and installation costs until the biometric air exit program is fully implemented nationwide, will incur added time burden costs to boarding agents as a result of longer boarding times per flight when conducting biometric collection at exit and will bear incremental training costs. CBP also expects the sea travel industry to incur costs from procuring additional facial comparison hardware as they continue to expand FBD operations and from training debarkation agents on how to properly conduct FBD operations. As shown in Table 3, CBP estimates the total costs during the regulatory period will be approximately \$792 million in undiscounted 2024 U.S. dollars or on average \$158.5 million annually.

During the regulatory period CBP expects that CBP, inbound air travelers, and sea travelers will experience cost savings during the entry process from the use of facial comparison technology at Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry. CBP estimates that cost savings to CBP, inbound air, and sea travelers will be approximately \$505 million in undiscounted 2024 U.S. dollars or on average \$101 million annually during the regulatory period. CBP also anticipates that the sea travel industry will experience time savings during the debarkation process when conducting FBD operations resulting in around 1.25 hours of time savings per vessel arrival. CBP

¹⁸³ CBP notes that the actual time burden incurred during biometric collection at exit for outbound air travelers boarding non-CBP biometric flights could be less than CBP estimates in this analysis as restrictive COVID-19 health requirements ease, as boarding agents and travelers become more familiar with the facial comparison technology in the exit process and if enhancements to technology continue to be implemented making the process more efficient.

¹⁸⁴ CBP notes that actual time burden to the average inbound pedestrian traveler when processed through Pedestrian Entry is uncertain. CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times. Therefore, the actual time burden from implementing Pedestrian Entry could be less than CBP estimates in this final rule.

presents net costs for each year of the regulatory period in Table 3, and CBP estimates that total net costs during the regulatory period will be approximately \$287 million in undiscounted 2024 U.S. dollars, or on average \$57 million annually.¹⁸⁵

Table 3. Regulatory Period Projected Net Costs, FY 2025–2029 (undiscounted thousands of 2024 U.S. Dollars)

Fiscal Year	Costs	Cost Savings	Net Costs
2025	\$150,718	\$90,232	\$60,485
2026	\$164,062	\$97,642	\$66,420
2027	\$156,009	\$102,532	\$53,477
2028	\$159,360	\$106,033	\$53,327
2029	\$162,380	\$108,704	\$53,675
Total	\$792,528	\$505,144	\$287,385
Average Annual	\$158,506	\$101,029	\$57,477

Note: totals may not sum due to rounding

The primary benefit of this final rule is the enhanced security from having biometric confirmation using facial comparison technology of the identification of alien travelers entering and leaving the country to prevent imposters attempting to fraudulently enter the United States, identifying individuals who have overstayed their visas, and individuals who have entered the United States without inspection at entry. CBP is unable to monetize these security benefits in the analysis for the final rule. Comparing biometrics at entry and departure enables CBP to know with greater certainty the identity of those entering and leaving the United States, which will help detect and deter visa overstays and visa fraud; helps identify persons attempting to fraudulently use travel documents; and alerts authorities to criminals or known or suspected terrorists prior to

¹⁸⁵ CBP believes that net costs could be less than presented here due to the uncertainty surrounding the actual time burden incurred by outbound air travelers boarding non-CBP biometric flights and inbound pedestrians processed through Pedestrian Entry. CBP anticipates that the added time burden from conducting biometric collection for outbound air travelers boarding non-CBP biometric flights could be less or even result in a time savings in the future as restrictive COVID-19 health requirements ease, and as boarding agents and the traveling public become more familiar with the biometric collection process, and enhancements to the technology continue to be implemented making the process more efficient. At entry in the land environment CBP made changes to the primary inspection entry process for pedestrians after the implementation of facial comparison technology for biometric collection for Pedestrian Entry, which prevented CBP from separating the two effects and CBP was only able to identify the combined effect on pedestrian entry processing times.

entry or exit. For FY 2023, DHS estimates that about 565,155 aliens who entered by air or sea and were expected to depart that year overstayed their lawful period of admission, or 1.45 percent of aliens arriving by air and sea.¹⁸⁶ The implementation of facial comparison technology pilots has already yielded positive security benefits. The facial comparison technology pilots at exit have helped identify over 444,552 visa overstays and 12,669 individuals who previously entered the United States without inspection.¹⁸⁷ Additionally, since 2018, CBP facial comparison technology used at entry has detected over 2,000 imposters at ports of entry, who were using genuine travel documents when attempting to fraudulently enter the United States.¹⁸⁸

Table 4 presents monetized present value and annualized net costs for the final rule during the regulatory period.¹⁸⁹ CBP estimates total net costs from this final rule will range between around \$264 million and \$237 million over the regulatory period, using a three and seven percent discount rate. On an annualized basis, net costs will range within \$57 million. CBP notes that the actual net costs for this final rule could be less depending on how efficiently the air travel industry and sea travel industry can implement facial comparison technology for biometric collection and if the air travel industry is able to speed its processing as it moves past the pandemic environment.¹⁹⁰ CBP notes that the time-in-motion study was conducted during a time with COVID-19

¹⁸⁶ DHS, FY 2023 Entry/Exit Overstay Report 12 (2024), https://www.dhs.gov/sites/default/files/2024-10/24_1011_CBP-Entry-Exit-Overstay-Report-FY23-Data.pdf (last visited May 19, 2025).

¹⁸⁷ Information provided by CBP's Strategic Transformation Office, Planning, Program Analysis, and Evaluation, Office of Field Operations, subject matter expert on January 31, 2023, and March 6, 2025.

¹⁸⁸ See CBP, Biometrics, <https://www.cbp.gov/travel/biometrics> (last modified April 16, 2025) (last visited May 21, 2025).

¹⁸⁹ CBP displays the net costs associated with only the regulatory period to show the effects of this final rule after it is implemented. The effects incurred during the pilot period are considered sunk costs and cannot be recouped. CBP will also display the net costs for these biometric programs as a whole from 2017-2029.

¹⁹⁰ CBP Time and Motion Study, conducted to determine the processing times for biometric collection at exit in the air environment, was conducted in 2021 when airport COVID-19 protocols were still in place. Therefore, CBP's estimates in this analysis for time burdens incurred during the biometric collection process at exit in the air environment may reflect a less efficient process than will occur in future years.

travel restrictions and that those may have lengthened both the baseline inspection process and the biometric inspection process. CBP expects that time burdens from using facial comparison technology for biometric collection at exit in the commercial air environment could have decreased or even became time savings now that COVID-19 restrictions have been lifted, boarding agents and travelers become more familiar with the technology and future enhancements to technology make the process more efficient. Additionally, the actual time burden to inbound pedestrians processed through Pedestrian Entry is somewhat uncertain and CBP anticipates it could be less than CBP presents in this analysis because CBP changed the entry process and policies after Pedestrian Entry was implemented, likely increasing the average entry processing time per inbound pedestrian. If efficiencies are gained over time to make the process less burdensome, net costs from this final rule could be significantly less during the regulatory period. The primary benefit of this final rule is improving CBP's national security efforts by validating the identity of aliens entering and exiting the United States.

Table 4. Total Monetized Present Value and Annualized Net Costs of Regulatory Period, 2025–2029 (thousands of 2024 U.S. Dollars)

	3% Discount Rate	7% Discount Rate
Present Value Net Cost	\$263,951	\$237,148
Annualized Net Cost	\$57,635	\$57,838

CBP also displays the total effect of this final rule as a whole from 2017-2029.

Table 5 below shows the total costs, cost savings, and net costs from the biometric collection programs using facial comparison technology, from 2017-2029 in undiscounted 2024 U.S. dollars. In total CBP estimates that this final rule will result in total costs of around \$1,625 million during the entire period of analysis (2017-2029). Average annual costs are estimated to be around \$125 million. Total cost savings from this final rule are expected to be around \$765 million or on average \$59 million annually.

CBP anticipates that the total net costs from 2017-2029 will be around \$860 million or on average \$66 million annually.

Table 5. Biometric Programs Costs, Cost Savings and Net Costs, 2017-2029 (undiscounted thousands of 2024 U.S. dollars)

Fiscal Year	Costs	Cost Savings	Net Costs
2017	\$91,818	\$0	\$91,818
2018	\$101,138	\$3,032	\$98,106
2019	\$124,484	\$12,770	\$111,714
2020	\$88,828	\$8,437	\$80,391
2021	\$73,592	\$18,019	\$55,573
2022	\$115,981	\$50,846	\$65,135
2023	\$117,240	\$77,355	\$39,885
2024	\$119,480	\$89,597	\$29,883
2025	\$150,718	\$90,232	\$60,485
2026	\$164,062	\$97,642	\$66,420
2027	\$156,009	\$102,532	\$53,477
2028	\$159,360	\$106,033	\$53,327
2029	\$162,380	\$108,704	\$53,675
TOTAL	\$1,625,090	\$765,201	\$859,890
AVERAGE	\$125,007	\$58,862	\$66,145

CBP also provides the monetized present value and annualized net costs for the final rule during the entire period of analysis (2017-2029) in discounted 2024 U.S. dollars. CBP estimates total net costs from this final rule will range between around \$722 million using a three percent discount rate and \$587 million using a seven percent discount rate. On an annualized basis, total net costs from this final rule will range from \$67 million using a three percent discount rate and \$70 million using a seven percent discount rate. In addition to the costs, cost savings and net costs, this final rule provides added national security benefits as discussed above. Table 6, below, displays CBP's estimates for the present value and annualized net costs from this final rule from 2017-2029.

Table 6. Biometric Programs Total Monetized Present Value and Annualized Net Costs, 2017 - 2029 (thousands of 2024 U.S. Dollars)

	3% Discount Rate	7% Discount Rate
Present Value Net Cost	\$722,151	\$587,300
Annualized Net Cost	\$67,904	\$70,271

B. *Regulatory Flexibility Act*

The Regulatory Flexibility Act (5 U.S.C. 601 *et. seq.*), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104-121, 110 Stat. 857), requires an agency to prepare and make available to the public a regulatory flexibility analysis (RFA) that describes the effect of a proposed rule on small entities (i.e., small businesses, small organizations, and small governmental jurisdictions) when the agency is required to publish a general notice of proposed rulemaking for a rule.

The Regulatory Flexibility Act requires agencies to consider the impacts of their rules on small entities. This final rule would only directly regulate individual travelers, who are not considered small entities. CBP received a public comment suggesting that individual travelers could be small businesses, sole proprietors, self-employed individuals, and freelancers, therefore a significant number of small entities would be affected as a result of this rule and that warrants a complete RFA for this rule. CBP does not have data on how many international travelers would fall in these categories. However, the effects on individual travelers are not significant. CBP estimates that the time burden to air travelers is less than 4-6 seconds (0.00167 hours) per boarding, or less than \$0.12 per individual traveler during the boarding process.¹⁹¹ Additionally, CBP estimates the average time burden to inbound pedestrians is approximately 15 seconds

¹⁹¹ 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.” CBP used the Department of Transportation (DOT) hourly wage rate for all-purpose air travelers, adjusted to 2024 values (\$65.69) to monetize the potential cost to the individual traveler, during the boarding process.

(0.00417 hours) per entry, or around \$0.12 per individual traveler during the entry process.¹⁹² The air travel and sea travel industry are indirectly affected by the final rule as the final rule does not place any requirements on travel industry members, and does not grant them any new rights. Any participation by air travel industry and sea travel industry members is strictly voluntary and CBP expects that air travel industry and sea travel industry members will only participate if they believe the benefits of participation outweigh the costs. CBP therefore certifies that this final rule will not result in a significant economic impact on a substantial number of small entities.

C. Unfunded Mandates Reform Act of 1995

This rule will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any one year (adjusted for inflation), and it will not significantly or uniquely affect small governments. Therefore, no actions are necessary under the provisions of the Unfunded Mandates Reform Act of 1995, Pub. L. 104-4, 109 Stat. 48.

D. Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3507), an agency may not conduct, and a person is not required to respond to, a collection of information unless the collection of information displays a valid control number assigned by OMB. The collections of information related to this final rule, including biometric exit, Simplified Arrival, FBD, Mobile Primary Face, and Pedestrian Entry are approved by OMB under OMB Control Number 1651-0138. CBP anticipates that this final rule would reduce the overall time burdens incurred by respondents during the information

¹⁹² 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.” CBP used the DOT hourly wage rate for all-purpose intercity surface travelers, adjusted to 2024 values (\$28.75) to monetize the potential costs to the individual pedestrian traveler during the entry process.

collection for biometric identity verification. The implementation of facial comparison technology for biometric collection is significantly quicker and more efficient than previous processes (e.g., collection of fingerprints). Because facial comparison technology generates a more efficient process, the time burden for an information collection response is expected to decrease.

However, this final rule would also introduce new time burdens to travelers departing the United States and CBP expects that the total number of travelers affected by biometric identity information collection will increase as a result of this final rule. Additionally, as CBP partners with air travel industry members and sea travel industry members, they will also incur some time burdens as a result of this final rule while they facilitate the collection of the biometric identity information. CBP assumes that the new time burden to conduct biometric identity using facial comparison technology is approximately 0.00095 hours (3.42 seconds) based on the CBP Time and Motion Study conducted on facial comparison technology implementation for biometric collection at exit in the air environment. CBP uses this estimate of 3.42 seconds for the average time burden to capture an image by facial comparison technology and conduct the biometric identity verification in all environments.

CBP estimates that the overall total time burden to the public from this information collection will decrease from around 705,336 hours to around 536,583 hours annually. Additionally, CBP anticipates that under this collection the total number of responses and respondents will increase from 115,200,000 to around 414,044,049. This information collection is being revised to reflect a reduction in burden hours and an increased number of travelers affected by facial comparison biometric collection as a result of this final rule. The new information collection requirements for this final rule will result in the following estimated time burdens to the public for information

collection under OMB Control Number 1651-0138 from expanding facial comparison technology for biometric identity for each environment below:

Biometric Data Fingerprint in all environments

Estimated number of respondents: 16,587,550

No. of Responses Per Respondent: 1

Total Responses: 16,587,550

Estimated time burden per response: 0.0097 hours (35 seconds)

Total estimated time burden: 160,899 hours

Biometric Exit Air Passenger Travelers

Estimated number of respondents: 98,982,807

No. of Responses Per Respondent: 1

Total Responses: 98,982,807

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 94,034 hours

Biometric Exit Air Travel Industry

Estimated number of respondents: 98,982,807

No. of Responses Per Respondent: 1

Total Responses: 98,982,807

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 94,034 hours

Simplified Arrival Air Passengers

Estimated number of respondents: 116,329,615

No. of Responses Per Respondent: 1

Total Responses: 116,329,615

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 110,513 hours

Simplified Arrival Sea Passengers

Estimated number of respondents: 947,878

No. of Responses Per Respondent: 1

Total Responses: 947,878

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 900 hours

Simplified Arrival Sea Crew Members

Estimated number of respondents: 365,479

No. of Responses Per Respondent: 1

Total Responses: 365,479

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 347 hours

Facial Biometric Debarkation Passengers

Estimated number of respondents: 10,124,005

No. of Responses Per Respondent: 1

Total Responses: 10,124,005

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 9,618 hours

Facial Biometric Debarkation Sea Travel Industry

Estimated number of respondents: 10,124,005

No. of Responses Per Respondent: 1

Total Responses: 10,124,005

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 9,618 hours

Mobile Primary Face Sea Crew Members

Estimated number of respondents: 378,782

No. of Responses Per Respondent: 1

Total Responses: 378,782

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 360 hours

Pedestrian Entry

Estimated number of respondents: 59,221,120

No. of Responses Per Respondent: 1

Total Responses: 59,221,120

Estimated time burden per response: 0.00095 hours (3.42 seconds)

Total estimated time burden: 56,260 hours

E. Privacy

CBP will ensure that all legal requirements (e.g., the Privacy Act, section 208 of the E-Government Act, and section 222 of the Homeland Security Act) and applicable policies are adhered to during the implementation of the biometric entry-exit system. All relevant privacy documents regarding the use of biometrics entry-exit technology are publicly available on DHS's Privacy website, <https://www.dhs.gov/privacy>.

CBP retains biographic records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, as provided in the DHS/CBP-007 Border Crossing Information (BCI) SORN.¹⁹³ Records associated with a law enforcement action are retained for 75 years as set forth in the DHS/CBP-011 TECS SORN.¹⁹⁴ CBP retains biographic entry and exit records in the Arrival and Departure Information System (ADIS) for lawful permanent residents and non-immigrant aliens,

¹⁹³ 81 FR 89957, 89962 (Dec. 13, 2016).

¹⁹⁴ 73 FR 77778, 77782 (Dec. 19, 2008).

consistent with the DHS/CBP-021 ADIS SORN.¹⁹⁵ Since 2004, CBP has collected biometric information in the form of fingerprints and a facial photograph on entry for in-scope travelers (pursuant to 8 CFR 235.1); CBP has transmitted this information to the DHS OBIM's IDENT, and may transmit this information to its successor information technology system, HART, currently in development, where it is stored and retained for 75 years as provided in the DHS-wide retention schedule for biometric records.¹⁹⁶

Under CBP's facial comparison-based entry-exit program, CBP's biographic data retention policies remain the same. CBP temporarily retains facial images of non-immigrant aliens and lawful permanent residents for no more than 14 days within Automated Targeting System (ATS)-Unified Passenger Module (UPAX) for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.¹⁹⁷ However, if the TVS matching service determines that a particular traveler is a U.S. citizen, CBP holds the photo in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage, and then deletes it.¹⁹⁸ Photos of all travelers are purged from the TVS cloud matching service within a number of hours, depending on the mode of travel.¹⁹⁹ Photos of in-scope travelers are transferred from ATS-UPAX and retained in IDENT and CBP systems for up to 75 years, consistent with existing CBP records that are housed in IDENT in accordance with the BCI SORN.²⁰⁰

¹⁹⁵ 80 FR 72081 (Nov. 18, 2015).

¹⁹⁶ See National Archives and Records Administration, Request for Records Disposition Authority, U.S. Department of Homeland Security, Biometric with Limited Biographical Data (2013), https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/departments-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

¹⁹⁷ TVS PIA at 21.

¹⁹⁸ TVS PIA at 21 & n.63.

¹⁹⁹ TVS PIA at 21.

²⁰⁰ See TVS PIA at 21.

CBP is implementing the biometric entry-exit system through the TVS. CBP has issued a number of PIAs for the TVS and earlier traveler verification tests,²⁰¹ which outline how CBP will ensure compliance with the DHS Fair Information Practice Principles (FIPPs)²⁰² as part of the biometric entry-exit system.²⁰³ In November 2018, CBP published the TVS PIA, a revised comprehensive PIA, which, along with the previous versions, examines the privacy impact and mitigation strategies of TVS as it relates to the Privacy Act and the FIPPs. The FIPPs address how information being collected is maintained, used and protected, particularly to issues such as security, integrity, sharing of data, use limitation and transparency.²⁰⁴ The comprehensive TVS PIA provides background information on early test deployments.²⁰⁵ Additionally, the TVS PIA explains throughout how CBP's use of facial comparison technology complies with privacy requirements at both entry and exit operations in all modes of travel where the technology is currently deployed. The TVS PIA is being updated in accordance with the regulations as revised by this final rule.

F. National Environmental Policy Act

DHS and its components analyze final actions to determine whether the National Environmental Policy Act of 1969 ("NEPA"), 42 U.S.C. 4321 et seq., applies to them and, if so, what degree of analysis is required. DHS Directive 023-01, Revision 01, and

²⁰¹ See DHS, DHS/CBP/PIA-056 Traveler Verification Service Related PIAs, <https://www.dhs.gov/publication/departure-information-systems-test> (last visited May 21, 2025).

²⁰² DHS, The Fair Information Practice Principles, <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles> (last visited May 21, 2025).

²⁰³ See, e.g., DHS/CBP/PIA-030, Privacy Impact Assessment for the Departure Information Systems Test (2016), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-dis%20test-june2016.pdf> (last visited May 21, 2025).

²⁰⁴ DHS, The Fair Information Practice Principles, <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles> (last visited May 21, 2025).

²⁰⁵ TVS PIA at 2-3.

Instruction Manual 023-01-001-01, Revision 01 (DHS Instruction Manual), establish the policies and procedures that DHS and its components use to comply with NEPA.²⁰⁶

NEPA allows Federal agencies to establish categories of actions (“categorical exclusions”) that experience has shown do not, individually or cumulatively, have a significant effect on the human environment and, therefore, do not require an environmental assessment (“EA”) or environmental impact statement (“EIS”). An agency is not required to prepare an EA or EIS for a proposed action “if the proposed agency action is excluded pursuant to one of the agency’s categorical exclusions.” 42 U.S.C. 4336(a)(2). The Instruction Manual, Appendix A, lists the DHS Categorical Exclusions. For an action to be categorically excluded, the DHS Instruction Manual requires the action to satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the Categorical Exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that would have or could create the potential for a significant environmental effect. DHS Instruction Manual, Section V.B.(1)-(3).

DHS analyzed this final rule and has concluded that the changes to 8 CFR parts 215 and 235 concerning the collection of biometric data from aliens upon entry and departure falls within DHS’s categorical exclusion A3. *See* DHS Instruction Manual, Appendix A, Table 1. Categorical exclusion A3 covers, among other things, the promulgation of rules that interpret or amend an existing regulation without changing its environmental impacts. First, the changes to 8 CFR parts 215 and 235 do not result in a

²⁰⁶ DHS, Directive 023-01, Rev. 01, Implementation of the National Environmental Policy Act (2014), available at https://www.dhs.gov/sites/default/files/publications/mgmt/environmental-management/mgmt-dir_023-01-implementation-national-environmental-policy-act_revision-01.pdf (last visited May 21, 2025); DHS, Instruction Manual 023-01-001-01, Rev. 01, Implementation of the National Environmental Policy Act (NEPA) (2014) (DHS Instruction Manual), available at https://www.dhs.gov/sites/default/files/publications/mgmt/environmental-management/mgmt-dir_023-01-implementation-national-environmental-policy-act_revision-01.pdf (last visited May 21, 2025).

change in environmental effect. Second, this final rule is a standalone rule and is not part of any larger action. Third, DHS is not aware of any extraordinary circumstances that would cause a significant environmental impact. Therefore, this final rule is categorically excluded, and no further NEPA analysis or documentation is required.

List of Subjects

8 CFR Part 215

Administrative practice and procedure, Aliens, Travel restrictions.

8 CFR Part 235

Administrative practice and procedure, Aliens; Immigration, Reporting and recordkeeping requirements.

Regulatory Amendments

For the reasons discussed in the preamble, DHS is amending 8 CFR parts 215 and 235 as set forth below:

PART 215—CONTROLS OF ALIENS DEPARTING FROM THE UNITED STATES; ELECTRONIC VISA UPDATE SYSTEM

1. The authority citation for part 215 is revised to read as follows:

Authority: 6 U.S.C. 202(4), 236; 8 U.S.C. 1101, 1103, 1104, 1184, 1185 (pursuant to Executive Order 13323, 69 FR 241, 3 CFR, 2003 Comp., p. 278), 1357, 1365a and note, 1365b, 1379, 1731-32; and 8 CFR part 2.

2. Amend § 215.8 as follows:

- a. Revise the section heading;
- b. Revise paragraph (a);
- c. In paragraph (b), add a paragraph heading and revise the first sentence; and
- d. In paragraph (c), add a paragraph heading.

The revisions and additions read as follows:

§ 215.8 Requirements for biometrics from aliens on departure from the United

States.

(a) *Photographs and other biometrics*—(1) *Photographs*. DHS may require an alien to be photographed when departing the United States to determine the alien's identity or for other lawful purposes.

(2) *Other biometrics*. DHS may require any alien, other than aliens exempted under paragraph (a)(3) of this section or Canadian citizens under section 101(a)(15)(B) of the Act who were not otherwise required to present a visa or have been issued Form I-94 (see § 1.4 of this chapter) or Form I-95 upon arrival at the United States, to provide other biometrics, documentation of immigration status in the United States, as well as such other evidence as may be requested to determine the alien's identity and whether the alien has properly maintained immigration status while in the United States, when departing the United States.

(3) *Exemptions*. The requirements of paragraph (a)(2) of this section shall not apply to:

- (i) Aliens younger than 14 or older than 79 on date of departure;
- (ii) Aliens admitted on A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas who are maintaining such status at time of departure, unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (a)(2) of this section;
- (iii) Classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or
- (iv) An individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not

apply.

(b) *Failure of a non-exempt alien to comply with departure requirements.* An alien who is required to provide biometrics when departing the United States pursuant to paragraph (a)(1) or (2) of this section and who fails to comply with the departure requirements may be found in violation of the terms of the alien's admission, parole, or other immigration status. * * *

(c) *Determination of overstay status.* * * *

PART 235—INSPECTIONS OF PERSONS APPLYING FOR ADMISSION

3. The authority citation for part 235 is revised to read as follows:

Authority: 6 U.S.C. 218 and note; 8 U.S.C. 1101 and note, 1103, 11f58, 1182, 1183, 1185 (pursuant to Executive Order 13323, 69 FR 241, 3 CFR, 2003 Comp., p. 278), 1185 note, 1201, 1224, 1225, 1226, 1228, 1357, 1365a and note, 1365b, 1379, 1731-32; 48 U.S.C. 1806 and note, 1807, and 1808 and 48 U.S.C. 1806 notes (title VII, Pub. L. 110–229, 122 Stat. 754); 8 U.S.C. 1185 note (sec. 7209, Pub. L. 108–458, 118 Stat. 3638, and Pub. L. 112–54, 125 Stat. 550).

4. Amend § 235.1 by revising paragraph (f)(1) to read as follows:

§ 235.1 Scope of examination.

* * * * *

(f) *Alien applicants for admission—(1) Requirements for admission.* Each alien seeking admission at a United States port-of-entry must present whatever documents are required and must establish to the satisfaction of the inspecting officer that the alien is not subject to removal under the immigration laws, Executive Orders, or Presidential Proclamations, and is entitled, under all of the applicable provisions of the immigration laws and this chapter, to enter the United States.

(i) *Permanent residents.* A person claiming to have been lawfully admitted for

permanent residence must establish that fact to the satisfaction of the inspecting officer and must present proper documents in accordance with [§ 211.1 of this chapter](#).

(ii) *Photographs*. DHS may require an alien seeking admission to be photographed to determine the alien's identity or for other lawful purposes.

(iii) *Other biometrics*. DHS may require any alien, other than aliens exempted under paragraph (f)(1)(vi) of this section or Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued Form I-94 (see § 1.4 of this chapter) or Form I-95 for admission or parole into the United States, to provide other biometrics, documentation of immigration status in the United States, as well as such other evidence as may be requested to determine the alien's identity and admissibility and/or whether the alien has properly maintained immigration status while in the United States.

(iv) *Failure to comply with biometric requirements*. The failure of an alien at the time of inspection to comply with paragraph (f)(1)(ii) or (iii) of this section may result in a determination that the alien is inadmissible under section 212(a) of the Immigration and Nationality Act or any other law.

(v) *Biometric requirements upon departure*. Aliens who are required under paragraphs (f)(1)(ii) or (iii) of this section to provide biometrics at inspection may also be subject to the departure requirements for biometrics contained in § 215.8 of this chapter, unless otherwise exempted.

(vi) *Exemptions.* The requirements of paragraph (f)(1)(iii) of this section shall not apply to:

(A) Aliens younger than 14 or older than 79 on the date of admission;

(B) Aliens admitted on A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (f)(1)(iii);

(C) Classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or

(D) An individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

* * * * *

Kristi Noem,
Secretary of Homeland Security.

[FR Doc. 2025-19655 Filed: 10/24/2025 8:45 am; Publication Date: 10/27/2025]