AMERICAN IMMIGRATION LAWYERS ASSOCIATION

December 30, 2025

Office of Policy and Strategy,
U.S. Citizenship and Immigration Service 5900 Capital Gateway Drive
Camp Springs, MD 20746

Submitted via http://www.regulations.gov

Re: **Comments on Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (DHS Docket No. USCIS-2025-0205)**

To Whom it May Concern:

The American Immigration Lawyers Association (AILA) submits the following comment in response to the Department of Homeland Security's (DHS) proposed collection and use of biometrics by U.S. Citizenship and Immigration Services (USCIS), as described in the Notice of Proposed Rulemaking, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services ("proposed rule" or "proposed biometrics rule").[1]

Established in 1946, AILA is a voluntary bar association of more than 18,000 attorneys and law professors practicing, researching, and teaching in the field of immigration and nationality law. AILA's mission includes the advancement of the law pertaining to immigration and naturalization and the facilitation of justice in the field. AILA members regularly advise and represent businesses, U.S. citizens, U.S. lawful permanent residents, and foreign nationals regarding the application and interpretation of U.S. immigration laws. The collective expertise and experience of our members make us especially well-qualified to offer comments on the proposed collection and use of biometrics by USCIS.

AILA strongly opposes the proposed biometrics rule because it would impose sweeping new requirements for noncitizens and all "associated"[2] U.S. citizens to turn over sensitive biometric data to the government (including DNA). If finalized, the rule will create new bureaucratic delays and threaten to create a surveillance state of "continuous vetting" for noncitizens as well as collect sensitive biometric data (including DNA) from U.S. citizens who are merely "associated" with

[1] 90 Fed. Reg. 49062 (Nov. 3, 2025).
[2] 90 Fed. Reg. 49062, 49064, footnote 7, defines "associated" as "a person with substantial involvement or participation in the immigration benefit request, other request, or collection of information, such as a named derivative, beneficiary, petitioner's signatory, sponsor, or co-applicant. The terms ''file,'' ''submit,'' ''associated with'' or variations thereof, as used throughout this rule, do not relate to attorneys and accredited representatives, although attorneys and accredited representatives may file or submit a request on behalf of a client. DHS, at this time, is not proposing biometrics submission by attorneys and accredited representatives."

AILA Doc. No. 25123132. (Posted 12/31/25)

noncitizens in the United States. This proposal is antithetical to basic American values. The proposed rule explicitly grants DHS authority to collect, store, and use biometric data, including DNA, from U.S. citizens who have any association with a petition or application for a U.S. immigration benefit.[3] The list of potentially impacted U.S. citizens includes not only immediate family members, but also extended family members,[4] those who serve as a financial sponsor, company representatives, those who write recommendation letters, Designated School Officials, and others. While we believe that identity verification is an important aspect of fraud detection, USCIS's extreme vetting proposal is contrary to the law, would do significantly more harm than good, and is not justified by the information provided in the rule. For all these reasons and the reasons detailed below, we urge the Department to withdraw the proposed rule.

Table of Contents

I. DHS'S ATTEMPT TO EXPAND THE DEFINITION OF "BIOMETRICS" TO INCLUDE THE COLLECTION OF PALM, PRINT, VOICE PRINT, IRIS IMAGE, OR DNA INFORMATION EXCEEDS THE STATUTORY AUTHORITY OF THE AGENCY 2

II. DHS HAS FAILED TO PROVE THAT THE CHANGES IN THE PROPOSED RULE ARE NECESSARY OR JUSTIFIED 5

III. DHS PROPOSES TO EXPAND THE DEFINITION OF BIOMETRICS SO THAT IT HAS THE AUTHORITY TO COLLECT FAULTY AND UNPROVEN MODALITIES WITH SIGNIFICANT PRIVACY IMPLICATIONS FOR CITIZENS AND NONCITIZENS ALIKE .. 6

IV. DHS'S EXPANSION OF UNIVERSAL BIOMETRIC COLLECTION BEYOND THE ARREST AND APPREHENSION CONTEXT IS A SIGNIFICANT EXPANSION OF PRIVATE DATA COLLECTION THAT LACKS CLEAR CONTROLS AND STRAYS FROM THE CIVIL NATURE OF IMMIGRATION PROCEEDINGS 13

V. EXTRAORDINARY CIRCUMSTANCES STANDARD TO RESCHEDULE BIOMETRICS APPOINTMENTS 14

VI. IMPACT ON VAWA SELF-PETITIONS AND T-1 ADJUSTMENT OF STATUS APPLICATIONS 14

VII. REUSE OF BIOMETRICS 17

VIII. CONCLUSION 21

I. DHS'S ATTEMPT TO EXPAND THE DEFINITION OF "BIOMETRICS" TO INCLUDE THE COLLECTION OF PALM, PRINT, VOICE PRINT, IRIS IMAGE, OR DNA INFORMATION EXCEEDS THE STATUTORY AUTHORITY OF THE AGENCY

[3] Proposed Rule, 90 Fed. Reg. at 49074, *see also* proposed 8 CFR 103.16(c)(1).
[4] 90 Fed. Reg. 11324 (Mar. 5, 2025).

In the proposed rule, DHS attempts to vastly expand the collection of biometric information in relationship to immigration benefit adjudication to include the collection of biometric data (including DNA) from U.S. citizens who may or may not be related to the non-citizen applicant or beneficiary. This goes far beyond the intent of Congress. In doing so, it exceeds statutory authority. To assess whether a government agency exceeded the statutory authority it holds, one must first determine "whether Congress has directly spoken to the precise question at issue."[5] Then, "the particular statutory language at issue, as well as the language and design of the statute as a whole," and the traditional tools of statutory construction should be used to determine whether Congress has provided an agency with authority to interpret a statutory duty.[6]

DHS claims it has "broad statutory authority to collect or require submission of biometrics" for people directly associated with a request for immigration benefits; and for purposes incident to apprehending, arresting, processing, and care and custody of aliens.[7] DHS first tries to ground that claim in the general authority to administer and enforce immigration laws charged to the Secretary of the Department of Homeland Security, citing Immigration and Nationality Act ("INA") section 103(a), 8 USC 1103(a).[8] The plain language of this general authority to pass regulations, however, does not provide any specific statutory authority to collect expansive biometric information.

The proposed rule notes that in recent years DHS "has adopted the practice of referring to fingerprints and photographs collectively as biometrics, biometric information, or biometric services."[9] Despite this well-established understanding, DHS is seeking to clarify and expand its authority to collect more than just fingerprints to include the authority to collect palm print, voice print, iris image, or DNA information.[10] According to DHS, the proposed rule would provide DHS with the flexibility to change its biometrics collection practices and policies to ensure that DHS can make adjustments necessary to meet emerging needs, such as national security, public safety, or fraud concerns; enhance the use of biometrics beyond national security and criminal history background checks and document production, to include identity management in the immigration lifecycle and enhanced vetting, to lessen the dependence on paper documents to prove identity and familial relationships and preclude imposters; and improve the consistency in biometrics terminology within DHS.[11]

To support this new, expansive definition of "biometrics," DHS cites only one statutory provision, 18 USC 1028(d)(7)(B), which references personal data, such as voice prints and retina or iris images, in the context of an expansive list of potential "means of identification" that may form the basis for federal identity theft and fraud crimes.[12] DHS provides no source within Title 8 of the U.S. Code for a definition of "biometrics"—a term DHS admits it has previously only used to refer to fingerprints and photographs.

---

[5] *Loper Bright Enters. v. Raimondo*, 603 U.S. 369 (2024).
[6] *Chem. Mfrs. Ass'n v. U.S. E.P.A.*, 919 F.2d 158, 162 (D.C. Cir. 1990).
[7] Proposed Rule, 90 Fed. Reg. at 49063.
[8] *Id*.
[9] Proposed Rule, 90 Fed. Reg. at 49066.
[10] Proposed Rule, 90 Fed. Reg. at 49067.
[11] *Id*.
[12] Proposed Rule, 90 Fed. Reg. at 49080.

Despite the assertion in the proposed rule, a definitional provision in an unrelated criminal law does not give DHS authority to first create a general requirement to vastly expand the scope of the term "biometrics" in the context of immigration law to include the collection of palm print, voice print, iris image, or DNA information of noncitizens as well as U.S. citizens. In fact, no such authority exists.

After providing general authority, DHS then proceeds to claim that it does have "the specific authority for DHS to collect or require submission of biometrics" (while simultaneously trying to redefine the term). In support of this contention, DHS cites 8 USC 1225(d)(3) for the authority "to take and consider evidence of or from any person touching the privilege of an alien… concerning any matter which is material and relevant to the enforcement of this chapter."[13] Both statutes provide authority to immigration officers to "to administer oaths and to take and consider evidence" but the statutes do not discuss the type of evidence to be taken and definitely does not go as far as defining biometrics. We believe that it is far jump from the broad statutory language to the specific forms of proposed evidence to be taken by DHS and USCIS when balanced against the concerns we raise.

Lacking any other specific statutory authority, DHS then cites several provisions of the INA that provide explicit authority to collect photographs from naturalization applicants and fingerprints for "the purpose of registering aliens."[14] Neither of these statutes mention the word "biometrics," nor do they authorize the collection of palm print, voice print, iris image, or DNA information. Nevertheless, the Department attempts to use those portions of Title 8 of the U.S. Code to justify the vast expansion of the meaning of "biometrics" in U.S. immigration law through the proposed rule.

When Congress, however, intends for DHS to collect "biometrics," it has stated as much. The sole use of the phrase "biometrics" included in Title 8 comes in a requirement for Customs and Border Protection to create a "biometric entry/exit" system for individuals traveling into and out of the United States.[15] The term appears nowhere else within Title 8. Thus, to date, Congress has limited the term only to explicit situations relating to national security and border control and has not clearly stated its intent to apply such an expansive term to regular migration and the adjudication of immigration benefits.

DHS cites other statutes in an attempt to find authority to justify the expansion of the collection of biometric information from individuals. First, DHS refers to an old statute authorizing the Immigration and Naturalization Service (INS), which preceded the creation of DHS, to collect fingerprints, and connects the fee for that collection to the modern biometric services fee collected by USCIS.[16] Again, if Congress intended to require the submission of more than fingerprints, however, it would have indicated as much. Then, DHS references statutes that negatively impact applicants for certain benefits if they have been convicted of a "specified offense against a

[13] Proposed Rule, 90 Fed. Reg. at 49070, citing section 287(b) of the INA as authority for this proposed rule.
[14] Proposed Rule, 90 Fed. Reg. at 49072.
[15] 8 USC 1365b ("Biometric entry and exit data system").
[16] Proposed Rule, 85 Fed. Reg. at 56347 (citing the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act of 1998, Title I, Public Law 105-119, 111 Stat. 2440, 2447-2448 (1997)).

minor,"[17] a violation that affects criminal and security related grounds of inadmissibility[18], violations that impact eligibility for asylum and refugee[19] and[20] that impact eligibility for TPS status. Finally, DHS refers to the general requirement that adjustment [21] status applicants be admissible[22] moral character." Again, none of these statutes mention the word "biometrics" nor the collection of palm print, voice print, iris image, or DNA information.

In a final attempt to justify the authority to vastly expand the amount and types of information collected from people who interact with DHS, the proposed rule references the USA PATRIOT Act[23] and the Intelligence Reform and Terrorism Prevention Act of 2004,[24] which direct DHS to utilize "biometric technology" to develop an entry-exit system and require DHS to complete a biometric data system.[25] This terrorism prevention justification for the expansion of biometrics collection offered by DHS works hand-in-hand with the references to background checks and secure document production.[26] But as explained above, these statutes only show that Congress knows how to grant the authority to collect biometrics and has not granted such authority in any other circumstance. Lastly, DHS attempts to justify its authority to collect palm print, voice print, iris image, and DNA information from U.S. citizens and lawful permanent residents who file family-based petitions "to determine if a petitioner has been convicted of certain crimes pursuant to the Adam Walsh Child Protection and Safety Act of 2006 (AWA).[27] Again, that statute does not mandate such biometric collection. However, even if this statute authorized such collection, it would be impermissible to expand such a collection beyond the specific petition.

As a result, the proposed rule is ultra vires and violates the Administrative Procedure Act (APA) as "contrary to constitutional right, power, privilege, or immunity" as well as that it is "in excess of statutory jurisdiction, authority or limitations, or short of statutory right."[28] DHS attempts to ground its authority to expand the definition and collection of "biometrics" in various statutes, but in doing so DHS repeatedly attempts to unlawfully reinterpret statutes against the clear intent of Congress.

II. DHS HAS FAILED TO PROVE THAT THE CHANGES IN THE PROPOSED RULE ARE NECESSARY OR JUSTIFIED

Under current policy, the submission of biometrics is mandatory only for individuals pursuing a specific subset of immigration petitions and applications. If DHS wishes to collect biometrics from individuals pursuing other immigration benefits, the Department must justify the request and notify

---

[17] INA 204(a)(1)(A)(viii), 8 USC 1154(a)(1)(A)(viii).
[18] INA 212(a)(2)-(3), 8 USC 1182(a)(2)-(3).
[19] INA 207(c)(1), 8 USC 1157(c)(a); INA 212, 8 USC 1182; INA 208(b)(2)(a), 8 USC 1158(b)(2)(a).
[20] INA 244(c)(2)(A)(iii)-(B), 8 USC 1254a (c)(2)(A)(iii)-(B).
[21] INA 245(a)(2), 8 USC 1255(a)(2); INA 209(b)(5), 8 USC 1159(b)(5).
[22] INA 316(a)(3), 8 USC 1427(a)(3).
[23] Pub. L. 107-56, 115 Stat. 354 (2001) (codified at note to 8 USC 1365a).
[24] Pub. L. 108-456, 118 Stat. 3638 (2004) (codified as amended at 8 USC 1365b).
[25] Proposed Rule, 85 Fed Reg. at 56348.
[26] *See Id*. (referencing 8 USC 1158(d)(5)(A)(i) and 8 USC 1732(b)(1).
[27] Proposed Rule, 85 Fed. Reg. at 56348.
[28] 5 USC 706(2)(B)-(C) (1966).

the individuals that biometrics are required. DHS now proposes flipping this presumption so that biometrics collection is always authorized, unless the agency waives the requirement, without meaningful analysis or justification.[29]

Serious constitutional concerns exist in the collection of personal data from U.S. citizens and noncitizens. As such, even where Congress has mandated collection of biometrics at entry and exit of the United States, the participation by U.S. citizens is voluntary.[30] The Fourth Amendment provides critical protections against the unlawful intrusion on privacy rights, and its protections apply to citizens and noncitizens alike. Limitations on privacy must serve a legitimate purpose. They must also be necessary and proportional, and they must represent the least intrusive option available in reaching that [31] DHS's Proposed Rule fails to meet this standard.

The Proposed Rule, as currently drafted, is incomplete. DHS claims that the sweeping changes in this Proposed Rule are necessary and justified as the current data it collects "possess inherent inconsistencies that could result in immigration benefits being granted to ineligible applicants or imposters."[32] The Department uses this claim as a justification for both its sweeping redefinition of "biometrics" and requirement to include iris scans, palm prints, images for the purpose of facial recognition, and even DNA,[33] and its proposed broad expansion of the pool of individuals subject to such biometrics collection.

While DHS claims that immigration benefits could be granted to people improperly under the current structure, it fails to provide any evidence or meaningful analysis to support its claim that fingerprints are less reliable for identity verification than iris scans, palm prints, and voice prints in justifying its proposed extraordinary expansion of biometrics collection. Such information is critical in affording the public a meaningful opportunity to analyze the Proposed Rule and its efficacy. Without providing such evidence, implementing a rule with such a broad reach would be improper.

III. DHS PROPOSES TO EXPAND THE DEFINITION OF BIOMETRICS SO THAT IT HAS THE AUTHORITY TO COLLECT FAULTY AND UNPROVEN MODALITIES WITH SIGNIFICANT PRIVACY IMPLICATIONS FOR CITIZENS AND NONCITIZENS ALIKE

DHS proposes to expand the definition of "biometrics" to mean "measurable biological (anatomical, physiological or molecular structure) or behavioral characteristics of an individual," and include a list of modalities of biometric collection which include by are not limited to facial

---

[29] Proposed Rule, 85 Fed. Reg. at 56340.

[30] *See* 90 Fed. Reg 48604, 48611 (Oct. 27, 2025).

[31] *See, e.g.*, Federal Bureau of Investigation, Domestic Investigations and Operations Guide (Sept. 28, 2016), at 4.1.1(listing the requirement that FBI agents "[e]mploy the least intrusive means that do not otherwise compromise FBI operations" as one of six "basic principles that serve as the foundation for all FBI mission-related activities"), available at: https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version

[32] Proposed Rule, 85 Fed. Reg. at 56340

[33] Proposed Rule, 90 Fed. Reg. at 49067.

imagery (digital image, specifically for facial recognition and facial comparison), prints (including fingerprints and palm prints), signature (handwritten), ocular imagery (to include iris, retina, and sclera), voice (including voice print, vocal signature, and voice recognition), and DNA (partial DNA profile).[34] The proposed rule defines DNA as deoxyribonucleic acid, which carries the genetic instructions used in the growth, development, functioning, and reproduction of all known living organisms.[35] As explained below, DHS's rationale for this expansion of biometric modalities is unsupported. In addition, DHS's failure to articulate or even speculate as to the specific costs to the agency of implementing each biometric modality makes it impossible to effectively comment on the rule's cost/benefit analysis.

a. DNA: The proposed rule alleges that the unreliable nature of the current document-based system needs to be revised to allow DHS express authority to require, request, or accept raw DNA or DNA test results, including partial DNA profiles, to establish genetic relationships or confirm biological sex where required, from relevant parties, such as applicants, petitioners, derivatives, dependents and beneficiaries.[36] Although the Association for the Advancement of Blood & Biotherapies ("AABB") states "DNA testing provides the most reliable scientific test available to resolve a genetic relationship,"[37] the current use of primary evidence such as marriage and birth certificates functions without substantial fraud or the substantial costs created by the proposed rule, and DHS provides no evidence to the contrary.

Under the proposed rule, DHS would collect DNA samples from individuals using buccal swabs that would then be either tested at a DHS facility or DHS authorized facility (locally by a Rapid DNA machine) or mailed to an AABB-accredited laboratory for testing.[38] DHS is in the process of funding the development of cost-effective Rapid DNA equipment to allow non-technical users with appropriate training to analyze the DNA of individuals in a field setting and receive reliable results in about an hour.[39] However, DHS has not secured funding and acknowledges that "cost-effective Rapid DNA equipment" does not yet exist at DHS facilities or authorized facilities. Without these theoretical Rapid DNA tests, buccal swap samples will need to be transported to AABB-accredited laboratories, thereby creating a greater strain on an already overwhelmed United States medical testing system. The estimated wait time for results from a typical AABB-accredited facility ranges from two to three weeks for similar tests currently used to verify genetic relationships.[40] These tests are only performed in rare instances, but the proposed rule would dramatically increase the number of tests performed by these facilities, and the wait time for results would likely also increase considerably.

The proposed rule fails to address the impact this increase in adjudication time would have on USCIS receipts or the agency's budget, or the effect that these testing-related delays could have on existing USCIS adjudication backlogs while DHS secures funding to development and implement these Rapid DNA test capabilities. One example of the impact of collecting more DNA

[34] Proposed Rule, 90 Fed. Reg. at 49066; *see also* Proposed Rule, 90 Fed. Reg. 49135 and proposed 8 CFR 1.2.
[35] Proposed Rule, 90 Fed. Reg. at 49135 and proposed 8 CFR 1.2.
[36] Proposed Rule 90 Fed. Reg. at 49079 and proposed 8 CFR 103.16(a)(1) and (d)(2)(i)(A), (B).
[37] Proposed Rule, 90 Fed. Reg. at 49078 (FN 58).
[38] Proposed Rule, 90 Fed. Reg. at 49078.
[39] *Id*. at FN 60.
[40] *See* About AABB Accreditation.

samples can be found in the FBI's 2024 budget request to Congress, in which it sought to increase its budget for processing DNA samples by nearly double, asking Congress for an additional $53.1 million, up from its current $56.7 million budget to enable the agency to keep pace with the more than 1.5 million DNA samples it has received from DHS non-citizen detainees since 2020.[41]

The proposed rule fails to describe how false negative, unexpected findings, or other unusual test results are to be handled and reported. While DNA testing is highly reliable, it is not flawless. Its credibility depends on strict adherence to scientific protocols, transparency in lab practices, and careful interpretation in legal and medical contexts. The biggest risks come not from the science itself, but from human mistakes, faulty equipment, and misuse of results. The proposed rule states that DHS intends to perform DNA testing at its own facilities using Rapid DNA equipment, but it does not provide sufficient information or detail about how DHS plans to ensure the integrity of the DNA data it collects, describe how scientific protocols will be established and enforced, and/or describe how DNA data will be protected from human error in collection, testing, or analysis. A false negative test result could potentially result in the loss of an individual's immigration status if the adjudicator interpreted the inaccurate test as evidence of fraud on the part of the applicant. Although DNA testing can be highly accurate, the sheer number of tests required by the proposed rule would inherently carry a risk of mistakes, wrongfully depriving an individual of their immigration status. If an individual is not provided means to contest a DNA test result, an erroneous result could lead to the denial of an immigration benefit, or deportation or worse in the case of some asylum applicants. The proposed rule fails to address the negative impacts of this dynamic, along with the possible deterrent effect it would create for potential applicants afraid of their DNA information being misused or inadequately protected by testing facilities and DHS.

DHS also fails to address the long-term privacy concerns of people, including U.S. citizens, who will be subject to biometrics collection that will allow DHS to use, store, and share DNA test results with other law enforcement agencies.[42] Notably, when DHS collects DNA samples, neither U.S. citizens or foreign nationals are afforded 4th Amendment Constitutional protection against unreasonable search and seizure because immigration proceedings are civil, not criminal in nature. However, DHS shares DNA samples with U.S. law enforcement agencies for use in criminal proceedings and investigations. In doing so, the U.S. government, through DHS, circumvents the normal constitutional protections afforded to U.S. citizens and foreign nationals alike when collecting DNA samples. This practice, which is well-documented and the subject of litigation,[43] raises serious questions about the U.S. government's intention to amass vast amounts of biometric data, including DNA from U.S. citizens as well as foreign nationals, to conduct mass surveillance of all people in the United States.

Since the initial programs to collect DNA from people convicted of serious violent crimes began in 1988, states and the federal government have steadily expanded the use of DNA collection

[41] *See* Steve Glaberson, Emerald Tse & Emily Tucker, *Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing*, Center on Privacy & Technology at Georgetown Law (2024) at p. 20, available at https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/

[42] Proposed Rule, 90 Fed. Reg. at 49080.

[43] *See* DHS Collecting DNA as Part of Larger 'Massive Surveillance' Effort: Lawsuit - Newsweek

throughout the criminal justice system.[44] Under the AWA, the federal government may collect DNA samples from individuals "detained under the authority of the United States."[45] The Department now purports to carry over the steady expansion of DNA collection by the federal government into the civil immigration context.[46] The proposed rule claims the DNA test results are valid indefinitely, while failing to address the privacy concerns of people subject to the DNA collection policy when history suggests that future laws will continue to expand the use of DNA evidence throughout the federal legal system.[47]

b. Facial recognition: DHS proposes to expand biometrics collection to include photographs for specific use in facial recognition[48]. Despite rapid technological developments, significant concerns remain regarding the accuracy of facial recognition that undermines its stated purpose, as well as the secondary uses for such data.

DHS claims that facial recognition will assist the Department in determining if an applicant is who they claim to be but fails to provide any analysis or explanation of the purported benefits of facial recognition beyond those available through the current collection of fingerprints and photographs.[49] While the proposed rule indicates that facial recognition could be used to verify identity where fingerprints are unobtainable subsequent to the initial biometric enrollment at an Application Support Center (ASC), it does not provide any information regarding the proportion of such fingerprints that become unobtainable in this manner. Such data is necessary for stakeholders to meaningfully analyze the purported benefits of subjecting millions of people to unproven and highly invasive technology on an annual basis beyond what could already be sufficient.

The nature of facial recognition technology makes it highly susceptible to secondary uses and potential abuse. When combined with public video cameras, facial recognition technology can be used as a form of general surveillance. Moreover, it can be used in this manner passively and without the knowledge or consent of the parties impacted. When integrated with data from other governments and other government agencies, the collection practices proposed in this rule could allow DHS to build a database large enough to identify and track all people in public places, not just places DHS oversees, without their knowledge. Despite these concerns, the proposed rule does not provide any information regarding safeguards to prevent secondary uses and potential abuses.[50] The proposed rule fails to justify why such further measures are needed when weighed against the privacy concerns of those subject to these collections.

---

[44] *See* Steve Glaberson, Emerald Tse & Emily Tucker, *Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing*, Center on Privacy & Technology at Georgetown Law (2024) at p. 20, available at 2024.5.21_Raiding the Genome_full report_FINAL.pdf

[45] 42 USC 14135a(a)(1)(A).

[46] *See* Steve Glaberson, Emerald Tse & Emily Tucker, *Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing*, Center on Privacy & Technology at Georgetown Law (2024), available at https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/

[47] *See* Trump's DNA collection from immigrants sparks lawsuit over privacy concerns

[48] Proposed Rule, 90 Fed. Reg. 49082.

[49] *Id*.

[50] *See* GAO Report to Congress, Biometric Identification Technologies, Considerations to Address Information Gaps and Other Stakeholder Concerns (April 2024), available at https://www.gao.gov/assets/d24106293.pdf

c. Voice prints: DHS proposes expanding biometrics collection to include voice prints. In support of this proposal, DHS claims that the collection of voice prints will assist in improving the services provided by its call centers.[51] The proposed rule states that voice prints will help reduce concerns regarding a caller's identity and that individuals will more effectively be able to call for assistance or inquire about the status of a pending immigration benefit request.[52] DHS further claims that voice prints will help to identify indicia of fraud, screen for public safety or criminal history, and vet potential national security issues.[53] DHS fails to demonstrate a reasonable need to collect voice print as part of the process to determine if an individual is eligible for the benefit request sought.

DHS fails to provide any meaningful analysis to support these claims and to justify the invasive practice of creating and storing recordings of individual voices in perpetuity. Collecting and storing such features raise concerns that warrant careful consideration. Unprecedented new surveillance regimes must be supported by detailed explanations that ensure that DHS has grappled with the significance of its actions, not cursory remarks, and vague commentary. Moreover, serious questions remain regarding the overall efficacy and security of voice print technology that undermine DHS's stated justification. Just because such technology exists does not warrant use of the technology without careful consideration of its benefits and risks.

A study by Pindrop, a leader in the field of voice print technology, analyzed changes in voices over time found that an individual's voice experiences slight changes in speed and pitch over months and years.[54] While these subtle changes are not necessarily obvious to the human ear, they can negatively impact voice detection technology. The study found that error rates in voice biometrics can double over just a two-year period.[55] These results are not surprising given that the human body can use as many as 100 different muscles while speaking and the fact that our muscles weaken as we age.[56]

Additionally, the proposed rule fails to address other considerable security concerns associated with voice print technology. Experts indicate that technologies exist that are capable of emulating voices easily and can fool voice print platforms, especially where potential imposters are able to obtain fragments of the actual person speaking.[57] It appears that USCIS proposes to create a system in which individuals could access confidential data by phone through the collection of voice prints. Given the ubiquity of podcasts, YouTube videos, voicemails, and the like, the ability to regenerate

---

[51] Proposed Rule, 90 Fed. Reg. at 49082.
[52] *Id*.
[53] *Id*.
[54] *See* Jonathan Keane, Study Accuracy of Voice Biometrics Can Diminish as We Age, Digitaltrends, February 23, 2017, available at https://www.digitaltrends.com/computing/voice-biometrics-accuracy/.
[55] *Id*.
[56] *See* Frank H. Guenther and Gregory Hickok, Neural Modes of Motor Speech Control, Neurobiology of Language, 2016, https://www.sciencedirect.com/topics/medicine-and-dentistry/speech-production#:~:text=58.1%20Introduction,laryngeal%2C%20and%20oral%20motor%20systems.
[57] *See* Voice Biometrics Disadvantages & Vulnerabilities | Seeking Alternatives | iProov; *see also* 56 See Rupert Jones, Voice Recognition: is it really as secure as it sounds?, The Guardian, September 22, 2018, available at https://www.theguardian.com/money/2018/sep/22/voice-recognition-is-it-really-as-secure-as-it-sounds , *see also* FBI warns senior US officials are being impersonated using texts, AI-based voice cloning | Cybersecurity Dive, and https://www.ic3.gov/PSA/2025/PSA250515

an individual's voice, and therefore to compromise their security, creates a real concern that is entirely unaddressed by the proposed rule.

d. Palm prints: DHS proposes to expand biometrics collection to include palm prints. In support of this proposal, DHS states that it is "consistent with what the FBI has announced as part of its Next Generation Identification initiative for the development of an integrated National Palm Print Service, which would improve law enforcement's ability to exchange a more complete set of biometric information.[58] DHS fails to explain why USCIS, which is not a law enforcement agency, would need to assist the FBI with expanding their database of palm prints, or how it is within their statutory mission to do so. USCIS is not an investigatory agency, and immigration officers adjudicating benefits are not authorized to conduct domestic law enforcement. Nor would an individual's appearance in the National Palm Print Service generally affect eligibility for a benefit if the person had never been charged or convicted of a crime. DHS also does not explain what USCIS would do with palm print data or how the collection of palm print data would assist in the adjudication of immigration benefits other than a vague reference to background checks capability.[59]

DHS's complete failure to consider the cost/benefit analysis of collecting and storing palm print data indicates that DHS has not meaningfully considered or justified the collection.

e. Data retention: The privacy risks associated with biometrics databases are extreme, with the greatest concerns relating to the breach or loss of personally identifiable information (PII) and the risk of misuse for large-scale surveillance. The risk of such breaches or data loss relating to PII that DHS proposes to collect and store in perpetuity cannot be overstated. While the proposed rule makes passing references to related requirements that DHS maintain a robust system for biometrics collection, storage, and use related to providing adjudication and naturalization services, the proposed rule fails to specify how and where the department proposes to store the vast amount of PII that it proposes to collect. Specifically, the proposed rule states that biometric data will be stored in the Customer Profile Management System (CPMS) database, the USCIS data repository for biometrics information.[60] DHS also states that the biometric data can be processed and stored on other USCIS systems, but the proposed rule does not detail protocols in place to prevent breach or misuse of PII or name the other systems where data will be stored.

While DHS has historically stored biometric data in its Automated Biometric Identification System (IDENT),[61] this new data will likely be stored in IDENT's replacement: DHS's new Homeland Advanced Recognition Technology (HART) database.[62] HART is currently the world's second largest biometrics collection and storage system, and it is operated by DHS's Office of Biometric Identity Management and hosted by Amazon's GovCloud. According to HART's original privacy impact assessment, its records already include a wide array of information such as biometric data, biographic data, derogatory information such as warrants and immigration violations, officer

[58] Proposed Rule, 90 Fed. Reg. at 49081.
[59] *Id*.
[60] Proposed Rule, 90 Fed. Reg. at 49099.
[61] *See* https://www.dhs.gov/obim
[62] *See* https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1

comment information, encounter data, and other unique machine-generated identifiers.[63] DHS estimates that under the proposed rule, an additional 1.12 million new biometrics submissions will be collected annually, increasing the total number of biometric submissions from the current baseline of 2.07 million to 3.19 million.[64]

All this additional PII will presumably be stored in its HART database, combined with millions of other entries, and stored by a third-party contractor. If that is the case, the PII of millions of individuals impacted by this proposed rule will be vulnerable to breach or future misuse given that it will all be stored together in a single database using a unique identifier to link several different biometrics to each person forever. Moreover, the implementation of HART has been riddled with problems including numerous delays in implementation, ballooning costs, and major privacy protection concerns.[65]

DHS recognizes in the proposed rule that individuals could possibly be apprehensive about doing so and may have concerns germane to privacy, intrusiveness, and security.[66] DHS, however, refuses to consider the potential costs or likelihood of such a breach by dismissing the concerns by declaring that data security is an intangible cost. While we do not rule out the possibility that there are costs that cannot be monetized that accrue to aspects of privacy and data security, this does not warrant the failure to address the concerns.[67]

This failure to consider the costs and dangers of information security is not justified. In recent years, federal agencies, including DHS, have repeatedly failed to prove that they are capable of fully protecting PII and the significant risk of data loss has been made clear by several major breaches of federal databases, including breaches impacting millions of records in the last five years alone.[68] DHS must consider the costs of, and lessons learned from, these breaches when evaluating the proposed rule. Moreover, the consequences of such breaches often are not fully understood until years later, given their scale and the relatively minimal understanding among the public of the information contained in federal government databases. DHS's plans to move forward with a dramatic expansion of biometrics collection under these conditions, while refusing to conduct a thorough analysis of the anticipated costs and the likelihood of an information security breach, demonstrates a willful disregard of the privacy interests of millions of Americans and the impact that these breaches have on individuals.

---

[63] *Id*.
[64] *See* Proposed New Immigration Rule Seeks Expanded Biometric Data Collection, Including Voice and DNA, Across All Age Groups - NEPYORK
[65] *See* Grassley to DHS - HART Program Recommendations; see also Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy | U.S. GAO
[66] Proposed Rule, 90 Fed. Reg. at 49111.
[67] *Id*.

[68] *See* 11 Major Federal Data Breaches | Fortra; *see also* High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation | U.S. GAO and Hack of Contractor Was at Root of Massive Federal Data Breach, and Digital Deportation: DHS Surveillance That Could Fuel Trump's Plans for Mass Deportations

IV. DHS'S EXPANSION OF UNIVERSAL BIOMETRIC COLLECTION BEYOND THE ARREST AND APPREHENSION CONTEXT IS A SIGNIFICANT EXPANSION OF PRIVATE DATA COLLECTION THAT LACKS CLEAR CONTROLS AND STRAYS FROM THE CIVIL NATURE OF IMMIGRATION PROCEEDINGS

DHS's expansion of biometric information collection authority, particularly the changes to 8 CFR 236.5 regarding biometric collection following arrest or apprehension are of great concern because DHS does not address how this data will be stored, managed, shared, or protected from unauthorized disclosure in the proposed rule.

While AILA recognizes the importance of biometrics in immigration enforcement and identity verification, we are concerned that the proposed expansion risks blurring the lines between civil immigration enforcement and criminal law enforcement. Immigration proceedings are fundamentally civil in nature, yet the aggressive expansion of biometric collection authority including the removal of age limits and the broadening of use cases raises serious privacy and due process concerns.

Currently, 8 CFR 236.5 limits biometric collection to aliens aged 14 and older and to specific enforcement cases, with sharing of biometric data restricted to certain law enforcement agencies. The proposed rule removes the age restriction and authorizes biometric collection from all aliens subject to removal proceedings, expedited removal, reinstatement of removal orders, and other pathways, regardless of age. Additionally, the proposed rule authorizes DHS to collect biometrics, including DNA, from those "associated" with non-citizens who are arrested or apprehended and applying for U.S. immigration benefits, including U.S. citizens. This expansion significantly increases the population who are subject to biometric collection at or following arrest or apprehension and expands the scope of biometric data collection to include U.S. citizens who are associated with noncitizens' applications for U.S. immigration benefits.

Such a broadening of biometric collection authority risks subjecting vulnerable populations, including children under 14, to invasive data collection without clear safeguards. The removal of age limits is particularly troubling given the sensitive nature of biometric data and the potential for misuse or overreach.

Moreover, the proposed rule lacks sufficient clarity on the limits of data sharing and use of biometric information collected under these expanded authorities. Given the sensitive nature of biometric and genetic data, DHS must explicitly define and limit how this data can be shared with federal, state, local, and foreign agencies, and under what circumstances. Without clear boundaries, there is a risk of mission creep, where biometric data collected for civil immigration purposes could be used for unrelated criminal investigations or surveillance, undermining privacy rights, and due process protections.

In light of this, AILA urges DHS to:

1. Provide explicit, detailed limitations on data sharing, retention, and use of biometric information collected under 8 CFR 236.5 and related provisions, including transparency and accountability measures.
2. Maintain age restrictions on biometric collection, or at minimum, establish strict safeguards and justifications for collecting biometrics from minors.

3. Ensure that individuals subject to biometric collection have access to due process protections, including clear notice, the ability to challenge data collection or use, and remedies for misuse.

V. EXTRAORDINARY CIRCUMSTANCES STANDARD TO RESCHEDULE BIOMETRICS APPOINTMENTS

The expansion of biometric collection authority must be balanced with respect for privacy, civil liberties, and the distinct nature of civil immigration proceedings. The proposed rule states that if an individual fails to appear for a biometrics appointment "without good cause," they will lose their right to proceed with requested benefit. In addition, the proposed regulations state that for asylum applications or asylum related benefits, "good cause" requires a showing of "exceptional circumstances." Nowhere are these terms defined. We are concerned as to what qualifies as "good cause" or "exceptional circumstances." For instance, will someone who has been in an accident or in the hospital be permitted to reschedule their biometrics appointment if missed? Over the years, AILA members have reported that applicants have received biometrics appointments with very little notice, or the applicant never received the notice. If USCIS adopts the proposal to deny a benefit for failure to appear for a biometrics appointment, USCIS must establish clear guidelines that individuals will be given sufficient advance notice to arrange their schedules and travel to a biometrics appointment. We also recommend that USCIS explore options, including foolproof measures, to ensure proper delivering of notice to individuals.

This is particularly important for those in detention in light of the recent policy memo from USCIS.[69] In this policy memo, USCIS states that it is not permitted to enter jails, prisons, or non-DHS detention facilities to collect biometrics from detainees and USCIS does not have an agreement with ICE to collect biometrics for those detained who are not in removal proceedings with a U.S. immigration benefit request filed with EOIR. For example, how will biometrics be obtained for someone who is the beneficiary of a Form I-730, who has been detained but is not in removal proceedings with an application for relief filed with EOIR? Will the biometrics requirement be waived in this situation? If USCIS insists that biometrics be conducted in this situation, but USCIS does not provide a method to obtain biometrics or waive such requirement, USCIS will essentially keep a beneficiary from obtaining an approved I-730 and asylum as is required by law.[70]

Before USCIS terminates an application, it owes the application more articulate guidance and exceptions especially where failure to provide biometrics are due to circumstances created beyond the control of the applicant.

VI. IMPACT ON VAWA SELF-PETITIONS AND T-1 ADJUSTMENT OF STATUS APPLICATIONS

The proposed rule includes changes to good moral character requirements for VAWA self-petitioners and T-1 nonimmigrants applying for adjustment of status that are unnecessary, contrary

[69] *See* USCIS Policy Alert Issues Guidance on Biometrics for Individuals in Custody.
[70] INA 208(b)(3)(A).

to statute, and burdensome to both applicants and USCIS. The proposed changes increase the likelihood of prejudicial outcomes for survivors and undermine congressional intent behind creation of these special survivor protections. AILA urges USCIS to amend or withdraw the proposed changes as laid out below.

VAWA self-petitioners and T-1 nonimmigrant applicants for adjustment of status are required by statute to establish good moral character to be granted relief.[71] Per current 8 CFR 204.2(c)(2)(v), a VAWA self-petitioner must demonstrate, by any credible evidence, their good moral character during the 3-year period immediately preceding the filing of their self-petition. A child under 14 is presumed to be a person of good moral character.[72]

T-1 nonimmigrants applying for adjustment of status must demonstrate their good moral character during "a continuous period of at least 3 years since the date of admission" as a T nonimmigrant or "for a continuous period during the investigation or prosecution" of trafficking, "whichever period of time is less."[73] A child under 14 is presumed to be a person of good moral character.[74] Notably, and in recognition of the fact that trafficking victims are often forced or coerced to engage in criminal or other unlawful activity, the statute authorizes DHS to "waive consideration of a disqualification from good moral character . . . if the disqualification was caused by, or incident to, the trafficking."[75] USCIS will consider the applicant's credible evidence of good moral character.[76]

T applicants for adjustment of status are already required to complete biometrics as part of the application process.[77] VAWA self-petitioners are typically required to submit biometrics in order to receive an employment authorization document.[78]

Despite the existing statutory, regulatory, and policy framework, DHS has proposed a rule that (a) removes the presumption of good moral character for VAWA self-petitioners and T-1 adjustment applicants under 14 years old,[79](b) requires all VAWA self-petitioners and T-1 applicants for adjustment of status to complete biometrics, including those who are under the age of 14,[80](c) considers conduct beyond the requisite period immediately before filing, for both VAWA self-petitioners and T-1 nonimmigrants applying for adjustment of status, where: (1) the earlier conduct

[71] INA 204(a)(1)(A)(iii)(II)(bb) ("who is a person of good moral character"); INA 245(l)(1)(B) ("has, throughout such period, been a person of good moral character").
[72] *Id*.
[73] INA 245(l)(1); *see also* 8 CFR 245.23(a)(6) ("[h]as been a person of good moral character since first being lawfully admitted as a T-1 nonimmigrant and until USCIS completes the adjudication of the application for adjustment of status.").
[74] 8 CFR 245.23(g)(4).
[75] *See* INA 245(l)(6).
[76] 8 CFR 245.23(g)(3).
[77] *See* 7 USCIS-PM J.(3)(B) (T adjustment evidentiary requirements); DHS, *Adjustment of Status to Lawful Permanent Resident for Aliens in T or U Nonimmigrant Status*, 73 FR 75540 at 75553 (Dec. 12, 2008).
[78] *See* 10 USCIS-PM A.4(B) (identity verification requirements to be granted employment authorization); *see also* Proposed Rule, 90 Fed. Reg. at 49086.
[79] Proposed Rule, 90 Fed. Reg. at 49087-88 & 49089; *see also* proposed 8 CFR 204.2(v); and proposed 8 CFR 245.23(g)(4).
[80] Proposed Rule, 90 Fed. Reg. at 49086-87 & 49088; *see also* proposed 8 CFR 204.2(v); and proposed 8 CFR 245.23(g)(4).

or acts appear relevant to an individual's present moral character; and (2) the conduct of the self-petitioner/T-1 adjustment of status applicant during the three years immediately before filing does not reflect that there has been a "reform of character" from an earlier period,[81](d) requires all T-1 adjustment applicants to "submit evidence of good moral character as initial evidence" but does not clarify what that evidence is.[82]

The proposed changes are particularly problematic given that the T adjustment statute clearly lays out the period during which a T-1 applicant must demonstrate good moral character: during the three-year period following admission as a T nonimmigrant OR during the trafficking investigation or prosecution, whichever is less.[83] Permitting a look-back period pre-dating admission as a T nonimmigrant runs afoul of the statute and Congress' recognition that trafficking survivors should not be prejudiced by repeated adjudication of issues addressed during the T nonimmigrant stage through the discretionary waiver process.[84] The proposed rule's "reform of character" is extremely vague and introduces additional subjective elements that will likely lead to unjust denial of protections afforded under the law, as well as re-traumatization of the trafficking survivor or self-petitioner.

DHS is proposing amendments to the T adjustment good moral character requirement while leaving out a key statutory provision relating to acts caused by or incident to the trafficking that should not prevent a survivor from establishing good moral character. If USCIS is amending the regulatory good moral character requirement, it must do so while giving full effect to the statute. Amending the regulations to extend the period that may be considered when evaluating the applicant's good moral character without reference to the very relevant consideration that the trafficking may have caused certain conduct or events that USCIS may deem determinative of the applicant's good moral character will lead to unjust results that contravene congressional intent.

The good moral character evidentiary requirement for T-1 adjustment applicants is less clear under the proposed rule, indicating that applicants must submit evidence of their good moral character without specifying what evidence should or could be submitted while simultaneously removing the existing evidentiary requirements (i.e., police clearance letters and the applicant's affidavit). If USCIS updates the good moral character requirements for T-1 adjustment of status applicants, it should do so such that the requirements are clearer, not less so. Requiring biometrics of all VAWA self-petitioners and T-1 adjustment of status applicants under the age of 14 would lead to the absurd result of mandating that toddlers and young children appear for biometrics to purportedly assess their good moral character even though they are highly unlikely to have had interactions with the criminal legal system.

---

[81] *See* Proposed Rule, 90 Fed. Reg. at 49087 & 49089 (*referencing* 8 CFR 316.10(a)(2), pertaining to good moral character requirements at naturalization).

[82] *See* proposed 8 CFR 245.23(g)(4); Proposed Rule, 90 Fed. Reg. at 49069.

[83] INA 245 (l)(1)(B).

[84] *See* INA 245(l)(2), "A T nonimmigrant . . . shall be eligible to apply for adjustment of status . . . and the waiver . . . shall apply to any ground of inadmissibility which was waived in connection with the application for T nonimmigrant status." See also

The impact of USCIS's proposed expansion of the biometrics requirement to all VAWA self-petitioners and T-1 adjustment of status applicants will be exacerbated by the policy announced by USCIS on December 5, 2025 indicating that ICE has no obligation to collect biometrics from a noncitizen currently in ICE custody unless the individual is in removal proceedings and has an application or petition pending before EOIR.[85] Some VAWA self-petitioners and T-1 applicants for adjustment of status may be detained due to orders of removal and not in removal proceedings before EOIR, and some may be in removal proceedings before EOIR but will not have relief pending before EOIR. The net result of USCIS's new detained biometrics policy will be to bar an entire subset of survivors from accessing the protections afforded to them by Congress. If USCIS proceeds with the expansion of the biometrics requirement to all VAWA self-petitioners and T-1 applicants for adjustment of status, young children will be among those precluded from seeking the relief for which they are eligible. As mentioned above, USCIS must make allowances for those you are not able to provide biometrics due to circumstances beyond their control.

These proposed changes to the good moral character assessment for VAWA self-petitioners and T-1 adjustment applicants undermine the humanitarian nature of these remedies, as well as the many special statutory and policy protections for survivors of domestic abuse and trafficking. They create what is certain to be a higher bar for establishing good moral character, with greater reliance on subjective determinations by adjudicators and less clarity as to how the self-petitioner or applicant can demonstrate their eligibility. AILA respectfully urges DHS to withdraw these provisions that create confusion, increase barriers, and do not reflect serious consideration of the impact on vulnerable immigrant victims.

VII. REUSE OF BIOMETRICS

In the proposed rule, DHS recognizes the benefits and cost savings of reusing already collected biometrics. However, as proposed, the rule would limit reusing biometrics only to "positive biometric-based identity verification of fingerprint or 1:1 facial recognition matches," and only at DHS' discretion.

AILA supports reusing existing biometrics, and in particular, expanding the criteria for reuse of biometrics in order to reduce the burdens and costs on applicants and DHS staff over the costs involved with repeated biometrics collection.

While DHS recognizes that in many cases, collecting biometrics anew may be redundant, in order to retain its discretion to reuse prior biometrics for benefit requests submitted after an earlier one, DHS proposes only allowing reuse when these narrow criteria are met:

1. There is a positive biometric-based identity verification such as a fingerprint match or a 1:1 facial recognition match.
2. For previously collected fingerprints, reuse would still require an in-person identity verification at a DHS ASC.
3. For photographs, reuse may be allowed via biometric verification (e.g., approved facial comparison) rather than always requiring a new photo at each appointment.

[85] *See* USCIS, *Biometrics Collection for Aliens in Custody*, PA-2025-28 (Dec. 5, 2025).

4. Reuse cannot be based solely on non-unique biographic data (e.g., name, date of birth, or address).
5. Once collected, biometrics, other than DNA, may be stored and used or reused by DHS to conduct background checks; verify identity in subsequent encounters; produce secure documents such as permanent resident cards or travel documents; determine eligibility for benefits; or for other functions necessary to administer or enforce immigration and naturalization laws.[86]

The proposed rule discusses biometric reuse for "any individual who may have a pending benefit request or other request, or collection of information that requires biometric submission."[87] It does not define what "other request" is, nor what circumstances involve "collection of information that requires biometric submission."[88] The final rule should define what these mean for transparency purposes. AILA appreciates the examples given where USCIS will not require duplicative biometrics, such as for a combined filing of I-485 and I-601 applications. However, there are other circumstances where over an applicant's immigration lifecycle, the regulation seems to require duplicative biometrics collection numerous times. An example would be USCIS's recent announcement to reduce I-765 EADs for many categories from five years to 18 months, requiring biometrics every two years plus again for any other applications. Furthermore, "discretionary" reuse is not defined.[89]

In addition, DHS fails to show that repeated biometrics collection for "continuous vetting" is more cost effective than reusing already collected biometrics. Indeed, DHS's own statistics show that at least 39% of applicants were able to benefit from reuse of photographs, although no statistics were given regarding reuse of fingerprints.[90] Moreover, DHS has failed to show the number of actual or would-be criminals or terrorists who would have been discovered with the proposed continuous biometric collection and vetting to justify the expense and burden on the agency and on millions of other law-abiding applicants.

AILA proposes the following:

1. Allow exemptions for reuse where individuals prefer new captures.
2. Provide alternatives for those uncomfortable with facial comparison technologies. If facial recognition is used, allow an opt-out in favor of in-person identity verification. For instance, those whose appearance has changed due to medical treatment, gender transition, or significant aging may want new biometrics to avoid mismatches.
3. Since State Department applicants abroad already undergo rigorous biometric collection protocols, they should be reused for future immigration benefits, reducing duplicative captures, considering DOS and DHS share information through IDENT. Similarly, other

[86] *See* proposed 8 CFR 103.16(a)(4).
[87] 90 Fed. Reg. at 49067.
[88] *Id.*
[89] 90 Fed. Reg. at 49077.
[90] 90 Fed. Reg. 49062, 49102-49103, Table 5 and Table 6.

DHS collection agencies, such as ICE and CBP collect biometrics that can be reused by USCIS.[91]

4. Further, DHS should establish clear equivalency categories across form types that automatically qualify for reuse.
5. Reuse should be based on quality ratings of modern biometrics technologies for each capture rather than on chronology or quantity of application filings. In other words, reuse should be based on a high-quality previously collected set that is more reliable than requiring constant and potentially low-quality sets.
6. The NPRM should require independent audits of match accuracy or should define acceptable error rates.
7. AILA proposes expanding the criteria for reuse from solely positive biometric-based identity verification **(**for example, a fingerprint match or a 1:1 facial recognition match), to allow reuse for a fixed period of years for stable biometrics (e.g., fingerprints, iris scans). This reduces redundancy while still allowing periodic refresh for aging and/or other events (e.g., surgery).

In sum, by promoting reuse of stable biometrics already collected whenever possible, such a rule will foster the following benefits to applicants and to DHS:

- **Reduces burdens:** Fewer ASC appointments means that USCIS will need to expend fewer resources and focus on other priorities. Moreover, applicants will not have to take time off work, arrange childcare, travel long distances, or incur transportation costs all of which are particularly burdensome for elderly applicants, people with disabilities, those in rural areas far from an ASC, and low-income families who are more likely to be penalized for taking time off work. For many benefit types (e.g., adjustment, I-90, N-400, I-751), applicants may otherwise attend *multiple* biometrics appointments over the years of their immigration journey.
- **Speeds processing:** Reuse reduces appointment scheduling delays, staffing and contractor burdens, and background-check duplication, allowing USCIS to meet processing time goals.
- L**owers costs:** Reuse allows USCIS to redirect resources to reducing backlogs, staffing interviews, improving fraud detection, and modernizing digital systems. This benefits the agency and the public.
- **Minimizes duplicative collection:** If fingerprints or other biometrics are already on file and generated a **clear background check**, repeating the capture often adds no new information. For stable biometrics (e.g., fingerprints after adulthood, photos/facial recognition), repeat collection rarely provides additional identity-verification value. Reuse, therefore, preserves investigative resources for higher-risk cases.
- **Improves accuracy:** Biometric capture is prone to poor-quality fingerprints, dry or worn fingerprints, motion blur in photos, inconsistent lighting during capture, and racial bias

[91] Coincidentally, on December 5, USCIS announced it will not collect biometrics from applicants who are detained in removal proceedings, thus causing an automatic denial of benefits pending before USCIS. This seems to contradict the spirit and intent of this NPRM and to illegally force detainees to give up benefits they may be entitled to seek. https://www.uscis.gov/newsroom/alerts/uscis-updates-policy-on-biometrics-for-detainees

among other issues. However, when a high-quality, previously validated biometric exists, reuse can be **more accurate** than re-capturing at subsequent multiple appointments.

- **Reduces unnecessary appointments:** Reuse of stable biometrics allows USCIS to conserve time and resources and redirect its efforts toward other operational priorities. Requiring re-collection can be especially difficult for elders with mobility challenges, people with medical issues making fingerprinting painful; survivors of trauma who may prefer fewer government interactions, and children, who struggle with repeated appointments. Reuse is a more humane, trauma-informed approach. In addition, reuse is more equitable for those with transportation issues and job insecurity not faced by wealthier applicants.
- **Targets risk-based, rational, and efficient use of government resources:** preserves government resources for identity anomalies, fraud indicators, cases involving criminal background concerns, national security flags.
- **Aligns with OMB guidance and broader federal IT priorities:** reduces paper processes, decreases in-person burdens, increases automation (while preserving security), and streamlines benefit adjudication.

However, these burdens and cost benefits to applicants and the agency must be balanced with a commitment to protecting privacy, transparency, and civil liberties. AILA proposes the following changes to the NPRM:

1. Reuse should be limited to immigration benefit adjudications, identity verification, and fraud prevention. By contrast, continuous monitoring unrelated to an active benefit request can lead to mission creep, especially when used across agencies, which AILA opposes.
2. The rule should adopt a clear timeline for reuse.
    a. The rule does not appear to guarantee a clear expiration or deletion policy. Retaining biometrics indefinitely (or for decades) without clear limits undermines data minimization principles.
    b. Knowing that biometrics can be reused for unspecified future actions may deter people from applying for benefits, or foster fear among immigrant communities (especially if combined with enforcement). Such a policy erodes trust and promotes fear in immigrant communities.
    c. Reuse should be limited to very specific, narrow, time-bounded uses, with strong data retention limits, transparency, and individual consent or opt-out mechanisms such as described below.
    d. As written, the regulation is silent about how long DHS intends to store collected biometrics, or whether individuals have any right to request deletion.
3. There should be strong data retention rules and time frames.
    a. For example, as mentioned above, limiting the reuse period to a fixed period unless biometrics may be covered by other rules or statutes. In other words, retention should be limited to the applicant's immigration/citizenship journey and not thereafter.
    b. Storage rules should <u>not</u> be based on "just in case" scenarios.
    c. Once the retention period expires, the government should provide formal notice to individuals that the retention period has ended.
4. Provide transparency and notice
    a. As is done now, provide notices to applicants when their biometrics will be reused.

b. DHS should publish annual statistics on reuse rates, errors, match quality, security, and how many criminals or terrorists it discovered due to reuse notices, or failure to require new biometrics.
c. Establish an OIG office or independent auditing agency to oversee biometrics implementation, including reuse of existing biometrics.
d. Include accuracy benchmarks, false positive/negative rates for each biometric technology used, demographic bias checks, and algorithm audits.
e. There should be an explicit requirement for informed consent from individuals for reuse — and for future uses beyond the immediate benefit request.

5. Security and Minimization Safeguards
    a. Encrypt all stored biometrics using industry-leading standards.
    b. Limit access to personnel with a documented need-to-know.
    c. Require audit logs for every instance where biometric data is accessed or reused.
    d. Prohibit export or secondary commercial uses of biometric data.

VIII. CONCLUSION

The proposed rule is ultra virus and unnecessary for the carrying out the agency's functions. It has failed to provide adequate justification for its sweeping changes and to consider the impacts on U.S. citizens and noncitizens alike. The proposed rule should be withdrawn in the interest of protecting privacy, preventing agency overreach, and reducing burdens on both the agency and impacted individuals.

AILA appreciates the opportunity to comment on this rule, and we look forward to a continued dialogue with USCIS on issues concerning this important matter.

Sincerely,

THE AMERICAN IMMIGRATION LAWYERS ASSOCIATION