epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

U.S. CITIZEN AND IMMIGRATION SERVICES

DEPARTMENT OF HOMELAND SECURITY

Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

[DHS Docket No. USCIS-2025-0205]

January 2, 2026

By notice published on November 3, 2025, The U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), proposes amendments to its regulations governing collection and use of biometric data.[1] This proposal (hereinafter the Proposed Rule) would allow USCIS to (i) require biometrics from anyone (regardless of age) filing or associated with an immigration benefit request or other requests or data collections; (ii) expand biometrics collected in alien arrests; (iii) define biometrics; (iv) codify requirements around reuse of biometrics and other data; (v) codify and expand DNA testing, use, and storage; (vi) excuse failure to appear at a biometric services appointment only under "extraordinary circumstances;" (vii) modify how applicants demonstrate good moral character; and (viii) clarify biometrics collection purposes.

The Electronic Privacy Information Center (EPIC) submits the following comments to oppose the Proposed Rule and urge USCIS to immediately rescind the rule. The call for comments

[1] *Notice of Propose Rulemaking: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 90 Fed. Reg. 49062 (Nov. 3, 2025) [hereinafter Proposed Rule], https://www.federalregister.gov/documents/2025/11/03/2025-19747/collection-and-use-of-biometrics-by-us-citizenship-and-immigration-services.

lists four topics for comments to address, first among them "whether the collection of information is necessary for the proper performance of the functions of the agency."[2] Based on the information presented in the proposal, the answer to this question is "no." While EPIC understands the need to confirm identity for many of the listed applications and services, there is no evidence that identity confirmation has been a significant problem using the personal data already collected by DHS nor that broad collection of biometrics would address any such problem to the extent they exist.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[3] EPIC also has a sustained interest in DHS's biometrics policies and practices.[4]

---

[2] Proposed Rule at 49118.

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2018-0029 (Oct. 26, 2018), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-Correspondence-Records.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket No. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf; Comments of EPIC to the Department of Homeland Security, Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), *available at* http://epic.org/privacy/1974act/EPIC-SORN- Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), *available at* http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the United States Customs and Border Protection; Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[4] *See, e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (Jun. 22, 2020) *available at* https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018) *available at* https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf.

I. USCIS's Proposed Rule to increase biometric data collection and use is a dangerous escalation.

USCIS's Proposed Rule includes regulatory amendments that would require biometric data submission for multiple procedural and benefit request forms.[5] This is a significant escalation of the substantial personal data collection already required from applicants. Requiring biometrics in these instances is not merely unnecessary – it is a marked divergence from current practice that increases the risks to the security of personal data collected and carries with it broad potential for abuse and misuse.

a. Biometric data is a distinct personal data category with distinct risks.

Biometric data typically includes physical (and sometimes behavioral) characteristics such as facial, iris, or fingerprints. Behavioral biometrics include handwriting, gait, or emotion detection and have been frequently demonstrated to be inconsistent and inaccurate.[6] Biometrics are generally considered more sensitive and require higher forms of protection than other forms of personal data because they are immutable, unique to an individual, and intrinsically linked to a person's physical self.

---

[5] *Id*.

[6] *See, e.g.,* James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game,* The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/5/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; Kate Crawford, *Artificial Intelligence is Misreading Human Emotion,* The Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/; Charlotte Gifford, *The Problem with Emotion-Detection Technology,* The New Economy (Jun. 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology; Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test,* The Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404; Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions,* SSRN, 1, 1 (2018), https://papers.ssrn.com/sol13/papers.cfm?abstract_id=3281765.

The very presence of biometric data makes databases targets for malicious actors because of the potential to use that data for unauthorized access, scams, harassment, impersonation, and more.[7] Indeed, because biometric data points are immutable (or, in the case of behavioral biometrics, involuntary), they are incredibly desirable targets. While protections or changes may be put in place when other forms of personal data are breached, biometrics remain an ongoing vulnerability once compromised. A person may be able to change their password, but they cannot change their face. Conversely, age, illness, disability, injury, and more can alter biometrics in such a way that identification fails, resulting in additional burdens and potential discrimination for individuals within those already marginalized groups.[8]

In addition, biometric data is also a prime target for misuse through secondary processing that does not match the initial justification for collection. Once DHS holds all this biometric information, other agencies, researchers, or even private companies may look at the dataset as an asset to exploit, ignoring the initial limited collection and use scope. Companies like ClearviewAI build their products off troves of face prints, many of which are illegally acquired.[9] As the FTC has previously noted, biometric information can be used in producing deepfakes to impersonate, defame, or harass individuals.[10]

---

[7] *See, e.g.,* Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Motherboard, VICE (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice; Parmy Olsen, *Faces Are the Next Target for Fraudsters*, Wall Street Journal (Jul. 7, 2021), https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828; Alex Hern, *Hacker fakes German minister's fingerprints using photos of her hands*, The Guardian (Dec. 30, 2014), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

[8] *See* "Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act," FTC at 5 (May 18, 2023).

[9] Robert Hart, *Clearview AI—Controversial Face Recognition Firm—Fined $33 Million For 'Illegal Database,'* Forbes (Sept. 3, 2024), https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/.

[10] "Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act," FTC (May 18, 2023).

b. Facial recognition is a particularly perilous technology that USCIS is proposing to recklessly expand.

Despite the dangers of facial recognition technology, DHS has continued to expand its use and implementation of the technology culminating in the Proposed Rule that would give the agency wide latitude to continue the expansion and use of facial recognition.

Facial recognition can be deployed covertly, remotely, and on a mass scale. Despite escalating use, well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers, particularly for face recognition, are lacking. Similarly, there are a lack of comprehensive legal safeguards in place to ensure transparency, oversight, and accountability regarding the use of biometrics and to restrict their use in ways that better protect privacy, civil liberties, and civil rights. Ubiquitous identification via facial recognition eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and increases security risks from data breaches. An individual's ability to control disclosure of his or her identity is an essential aspect of personal freedom and autonomy. The use of facial recognition erodes these freedoms.

It is no wonder that facial recognition is so prevalent in authoritarian countries. Over the past several years, Russia has greatly expanded its infrastructure of security cameras equipped with facial recognition capabilities.[11] This broad surveillance apparatus has been used to suppress political dissent, particularly from political activists opposing the current war in Ukraine.[12] Similarly, China has an extensive surveillance infrastructure of facial recognition-capable cameras.[13] China has used its vast facial recognition network to crush dissent and in particular to suppress the Uyghur ethnic

[11] Cameron Manley, *Russia's Boom in Facial Recognition Cameras To Crack Down On Dissent*, World Crunch (Oct. 25, 2023), https://worldcrunch.com/focus/russia-ukraine-war/russia-facial-recognition-system/.
[12] Lena Masri, *Facial recognition is helping Putin curb dissent with the aid of U.S. tech*, Reuters (Mar. 28, 2023), https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.
[13] Keena Alwahaidi, *'They can track people over time': Inside China's extensive surveillance network*, CBC (Dec. 8, 2022), https://www.cbc.ca/radio/thecurrent/china-surveillance-network-1.6677778.

minority population in China.[14] And China has not stopped at just facial recognition, they also collect DNA, iris scans, and voice prints from as many people as possible (including innocent people) in the name of dealing with crime.[15] And, like China, USCIS now plans to collect vast amounts of biometric data across various modalities (e.g. DNA, iris, and voice) from people with no connection to any crime.[16]

China and Russia's vast facial recognition surveillance apparatus it not just built on a network of extensive cameras, it is built on societal integration of face print use for identification. Like authoritarian governments, USCIS wants to continue to expand facial recognition use for identity verification. This expansion threatens to create a digital biometric ID with dangerous implications. Identity verification via facial recognition increases the likelihood of mission and function creep and, consequently, greater government surveillance. Indeed, Immigration and Customs Enforcement has already taken the facial recognition system created for Customs and Border Protection's (CBP) Biometric Entry-Exit program and used it in the field to indiscriminately identify people in order to try to obtain their immigration status.[17] The lack of comprehensive regulation of facial recognition virtually guarantees that USCIS's proposed expansions of facial recognition use will increasingly threaten privacy, civil liberties, and civil rights. DHS should refrain from any expansion of the use of facial recognition that is not explicitly authorized by Congress.

---

[14] Alfred Ng, *How China uses facial recognition to control human behavior*, CNET (Aug. 11, 2020), https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

[15] Isabelle Quian *et al.*, *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*, N.Y. Times (Jun. 21, 2022), https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

[16] [2025 NPRM]

[17] Joseph Cox, ICE Is Using a New Facial Recognition App to Identify People, Leaked Emails Shows, 404Media (Jun. 26, 2025), https://www.404media.co/ice-is-using-a-new-facial-recognition-app-to-identify-people-leaked-emails-show/.

II. USCIS's Proposed Rule to expand its collection and use of biometrics does not comply with DHS's Fair Information Practice Principles (FIPPs) and ignores the privacy risks.

USCIS intends to add new "modalities" to its definition of biometrics and greatly expand the agency's collection and use of biometrics. When DHS or its subcomponents collects new information, including new modalities of biometric information, it must comply with the FIPPs. The FIPPs are rooted in the fundamental privacy practices articulated in the Privacy Act of 1974 and are designed to reduce the risks posed by collection and aggregation of PII. Furthermore, these practices outlined in the Privacy Act are incorporated by reference into the Homeland Security Act of 2002, which requires an appointment of a privacy officer whose chief duties include:

> (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
>
> (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974….[18]

The FIPPs are the "foundational principles of privacy policy" for DHS.[19] If the proposed new collection violates the FIPPs, which they do, then the agency should not move forward with the collection.

a. DHS's FIPPs set benchmarks for data collection and use that USCIS's Proposed Rule fails to adhere to.

DHS's FIPPs memo outlines the core principles around which the department should structure its data collection practices.[20] The FIPPs comprise eight mandates: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability.[21] Importantly, the FIPPs "*must be considered whenever*

[18] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142(a)(1)-(2).
[19] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security Memorandum Number 2008-01, Dep't. of Homeland Sec. (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[20] *Id*.
[21] *Id.* at 3-4.

a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[22] While all the FIPPs are important, examining USCIS's failure to adhere to the principles of Data Minimization, Use Limitation/Purpose Specification,[23] and Security get to the core of the threats posed by the Proposed Rule's unchecked biometric data collection.

1. Data Minimization

To meet the principle of Data Minimization, "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."[24] This standard breaks down into a) necessity of collection and b) limited retention. DHS has only met this standard when the department has ensured that the data it collects is necessary for a legitimate purpose and has ensured that data is retained only long enough to complete that legitimate purpose.

2. Use Limitation and Purpose Specification

Use Limitation requires that DHS, "use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected."[25] To comply with the Purpose Specification principle, "DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used."[26] Purpose Specification also requires that the DHS "articulate the need for a particular collection of information."[27] Use Limitation defines

---

[22] *Id*. at 3 (emphasis added).
[23] Although these are separate principles, they function together as checks on oversharing and misuse of data.
[24] Teufel III, *supra* note 19, at 4.
[25] *Id*.
[26] *Id*. at 3.
[27] Dep't of Homeland Sec., *The Fair Information Practices at Work* (Jun. 2011), https://www.dhs.gov/sites/default/files/2024-01/Governing%20Privacy%20Policy%20-%20FIPPs%20Factsheet.pdf.

the outer bounds of acceptable use for data already collected. Failure to meet either standard defeats both. Purpose Specification governs the decision to collect data, while Use Limitation governs the department's handling and exploitation of that data once collected. When information is exploited beyond the legitimate, specific purpose it was collected for, then that information is overused and the Use Limitation principle has been violated. Failure to define the purpose and limit the use of biometric data collection may lead to mission creep, as discussed below.

3. Security

In order to meet Privacy Act requirements and protect individuals, "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."[28] This principle requires proactive and comprehensive steps to guard against the release of PII. Where DHS cannot guarantee the security of PII, the agency should not collect it. In cases where DHS already possesses PII that is at risk of breach, the department should delete it posthaste.

b. USCIS plans to collect several new biometric modalities, and expand the collection of others, without a clear purpose or sufficient privacy protections.

USCIS's current practice is limited to collecting "photograph[s], fingerprints, and signature[s] to conduct identity, eligibility, national security, and criminal history background checks."[29] Where DHS collects other biometric modalities, the department has been engaged in limited tests, has obtained the biometric voluntarily as in a submitted DNA sample, or has determined that a specific practice or regulation requires the use of additional biometrics.[30] USCIS's Proposed Rule would expand its practices to routinely collect palm prints, photographs for facial

[28] Teufel III, *supra* note 19, at 4.
[29] Proposed Rule at 49073.
[30] To be clear, this is not an endorsement of DHS's past practices which have often collected far more biometric information than is necessary to DHS's mission, resulting in real privacy harms.

recognition, voice prints, iris images, and DNA. While the department's past practices have been far from minimized, this new regulation would move USCIS's practices into the realm of mass, indiscriminate biometric information collection.

1. Palm Print

USCIS plans to collect palm prints in addition to fingerprints as standard practice, to align with the FBI's planned background check system.[31] USCIS has also suggested that it may use palm prints as an identifier for immigration benefit applications.[32] However, the department does not claim that it needs palm prints in addition to fingerprints as identifiers for immigration benefits. USCIS suggests that palm print collection would be helpful and "improve the overall accuracy of identification through criminal history records," but does not provide evidence that the agency is failing to capture unqualified benefit applicants because of the lack of palm prints.[33] While capturing palm prints may be "of increasing interest"[34] to the law enforcement community, the broad compilation and storage of biometrics for "law enforcement" use is not a sufficiently descriptive purpose. As with other modalities, sweeping up palm prints without a unique, limited justification risks over-use.

2. Photographs

DHS has generally used photographs for in-person identification. Although the agency has experimented with using facial recognition in pilots such as the Biometric Entry/Exit Program, such uses were not standard practice for all applicants. USCIS's proposal to maintain databases of photographs including distinguishing features and facial recognition capabilities on all applicants would substantially expand the department's current practices.

---

[31] Proposed Rule at 49081-82.
[32] *Id*. at 49080.
[33] *Id*. at 49081-82.
[34] *Id*. at 49081.

3. Voice Print

USCIS has not articulated a unique need to collect voiceprints distinct from other biometric modalities. The agency cites four potential uses of voice print matching: 1) electronic submission of immigration benefits applications, 2) voice identification of callers to USCIS call centers, 3) voice identification for remote adjudication interview, and 4) general fraud prevention and national security uses.[35] USCIS has suggested it could use "microphones installed in cell phones, desk phones, computers, and laptops" to record an individual's voice.[36]

USCIS is not even clear on what type of voice recognition the agency would use. The Proposed Rule identifies both active and passive voice identification as options but fails to consider the substantial privacy differences between them.[37] Active voice ID asks the user to say a passphrase each time she seeks to be identified and compares the voiceprint to a pre-recorded version of the phrase, a 1:1 matching approach.[38] Passive voice ID compares how an individual speaks generally to a pre-recorded sample. Passive voice ID is easily expanded beyond legitimate authentication functions to identify any recorded sample of an individual speaking. EPIC has consistently testified in favor of 1:1 matching technologies as substantially more privacy protective.[39]

USCIS's proposal to collect voice biometrics fails to meet the principle of Data Minimization as there are other identification technologies available, including those presently in use. The failure to identify active voice identification as a safer technology for the public fails both the principle of Data Minimization and Security. The broad purposes behind USCIS's Proposed Rule, including

---

[35] *Id*. at 49082.
[36] *Id*. at 49113.
[37] *Id*.
[38] Matt Smallman, *Good Call: the hybrid answer to voice authentication*, 2020 Biometric Tech. Today 10-12 (2020), https://doi.org/10.1016/S0969-4765(20)30051-5.
[39] *See* EPIC Statement on Face Surveillance to U.S. House Committee on Homeland Security (Feb. 5, 2020), https://www.epic.org/testimony/congress/EPIC-HHSC-FRT-Feb2020.pdf, *and* EPIC Statement on Facial Recognition to Massachusetts General Court Joint Committee on the Judiciary (Oct. 22, 2019), https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf.

general fraud prevention and national security interests, render voice ID vulnerable to over-use. Failure to implement strong use limitation, particularly if USCIS adopts passive voice ID, will contribute to mission creep if USCIS seeks to leverage a database of voiceprints beyond caller identification.

4. Iris Images

USCIS proposes to add iris images as a new biometric modality to collect at Application Support Centers and as mobile biometrics, include these in the IDENT biometric database, and use iris images in the adjudication process.[40] To justify collecting iris images for all applicants, USCIS cites the need to identify individuals missing hands or lacking fingerprints.[41] However current USCIS policy sufficiently covers these situations. Where an individual has only a partial set of fingerprints (e.g. is missing a hand), USCIS simply collects the partial prints.[42] In the rare situations where an individual has a permanent loss of fingerprints, USCIS may grant a waiver.[43] USCIS therefore justifies collecting a new biometric modality for all applicants based on the extremely limited need to identify a small class of individuals. The stated purpose of the collection is so much smaller than the intended use that USCIS's collection of iris images cannot in its current form comply with FIPPs guidance. Expanding the already massive IDENT database with more biometrics will not improve USCIS's functioning but does threaten individual privacy.

5. DNA

USCIS proposes for the first time to require DNA testing as evidence of a family relationship.[44] Immigrants are already required to provide bevy of documentary evidence, including

[40] Proposed Rule at 49081.
[41] *Id*.
[42] USCIS Policy Manual Volume 1 General Policies and Procedures: Part C Biometrics Collections and Security Checks, Chapter 2 Biometrics Collection C. – Fingerprint Waivers (Oct. 6, 2020), https://www.uscis.gov/policy-manual/volume-1-part-c-chapter-2.
[43] *Id*.
[44] Proposed Rule at 49066, 49078.

birth and marriage certificates, medical records, religious documents, and affidavits.[45] The department claims to protect privacy by classifying the raw genetic material as a distinct biometric modality which will only be used for the original purpose of submission.[46] However, USCIS intends to treat DNA test results as any other biometric modality, to be stored and shared for "adjudication purposes… or to perform any other functions necessary for administering and enforcing immigration and naturalization laws".[47] The extra privacy protections claimed by USCIS are an empty promise, protecting only raw genetic material, the mouth-swab or spit-sample, without protecting the sensitive information contained within a DNA test. A person's genetic code is widely understood to be among the most sensitive types of personal information.[48] USCIS claims that the partial genetic profile it produces, containing 16-24 genetic markers, "does not reveal medical or hereditary conditions."[49] However, recent advances in genetic science have revealed that the "junk DNA" used for DNA fingerprinting can reveal the presence of disease.[50] Even if USCIS is right, the privacy implications of DNA do not begin and end with medical conditions. Partial DNA profiles can reveal race and heredity as well.[51] Disclosure of DNA test results, even a partial analysis, exposes a unique biometric identifier capable of revealing medical conditions and sensitive information around race and heredity.

---

[45] *Id*. at 49066.
[46] *Id*.
[47] *Id*.
[48] *See, e.g.,* Brief for EPIC as Amicus Curiae, Maryland v. King, 569 U.S. 435 (2013), *accessible at* https://www.epic.org/amicus/dna-act/maryland/EPIC-Amicus-Brief.pdf (arguing in part that retaining "junk DNA" used in CODIS has substantial privacy implications); Anita LaFrance Allen, Genetic Testing, Nature, and Trust, 27 Seton Hall L. Rev. 887 (1997) (noting that DNA testing creates "the potential for social stigma, discrimination in employment, barriers to health insurance, and other problems.")
[49] Proposed Rule at 49079.
[50] *See, e.g., Sieving through 'junk' DNA reveals disease-causing genetic mutations*, Science Daily (Oct. 3, 2013), https://www.sciencedaily.com/releases/2013/10/131003142321.htm (finding nearly 100 genetic variants in non-coding DNA are implicated in the development of breast cancer).
[51] Felipe Queiros, The visibilities and invisibilities of race entangled with forensic DNA phenotyping technology, 68 J. of Forensic and Legal Medicine 101858 (Nov. 2019), https://www.sciencedirect.com/science/article/pii/S1752928X19300873#bib26.

USCIS's proposal flies in the face of the principles of Purpose Specification and Use Limitation. USCIS would extract DNA for the limited purpose of confirming a family relationship and then leverage that information across the entirety of its work, ignoring the FIPPs entirely. USCIS has further failed the principle of Data Minimization. If USCIS truly needs to collect DNA to verify a family relationship, the department can retain only the result of the analysis (e.g. match/no match) in its records.

In total, USCIS's new and expanded biometric modalities would collect up to seven different modalities from an applicant.[52] USCIS would then have a stunning amount of information about the individual, down to a partial DNA profile, stored in the department's databases. USCIS does not and cannot need all of this information to identify an applicant for immigration benefits.

III. USCIS fails to justify the Proposed Rule while using it as a pretext to implement an overbroad and intensive surveillance regime that makes immigration more onerous and less desirable while disregarding the privacy and security costs and risk.

This rulemaking is clearly pretextual. The administration has repeatedly used scare tactics to smear immigrants, particularly those from central America. The administration has referred to these immigrants as rapists, criminals, and even terrorists for the mere act of wanting a better life for themselves in the United States.[53]

This has created an over inflated sense of fear relating to immigrants, which is then used to justify overly intrusive surveillance tactics like the oppressive biometrics regime in the USCIS Proposed Rule. USCIS proposes to expand the collection of biometric information both in kind (expanding the definition of biometric data to include facial recognition prints, voice recognition

[52] This assumes DHS would collect fingerprints, palm prints, signature, iris images, facial photographs, and voice prints for most if not all applicants, and that DHS here also required DNA.
[53] *See*, *e.g.,* Anna Betts, *From 'criminals' to 'garbage', Trump is ramping up anti-immigrant language*, The Guardian (Dec. 6, 2025), https://www.theguardian.com/us-news/2025/dec/06/trump-anti-immigrant-language.

prints, DNA, and more) and in scope (expanding collection to include minors from 0-14 years old and a broader set of U.S. citizens and permanent residents).

USCIS argues that this increase in collection would be to (1) facilitate identity management and (2) enhance the vetting of immigrants throughout the immigration process. In creating this onerous regime, USCIS explicitly changes the norm from using documentary evidence such as legal documents, including documents created by USCIS itself, with biometric verification providing back up support in cases where documentary evidence is not available.[54] Now, USCIS proposes a system where biometric verification is the primary form of identity management and background check information, where legal documents and other demographic information can be used at the discretion of USCIS officials as a secondary form of identification.[55]

To justify this unprecedented and overbroad expansion of biometric data collection, USCIS cites to purported fraud in individuals sponsoring fraudulent family members, individuals falsifying gender, imposters within the immigration process, and efforts to streamline the USCIS immigration process.[56] However, USCIS cites to few metrics that would substantiate any of these claims. In fact, several factors within the rulemaking directly contradict the claims made by USCIS, particularly in regard to efficiency and cost saving measures.

a. USCIS fails to substantiate claims of fraud and efficiency to support the agency's proposed draconian biometric collection measures.

There is no substantiation of USCIS' claims of fraud that would render DNA checks critical to USCIS's mission. The rulemaking broadly but vaguely refers to the need to reduce fraud and increase security on background checks, particularly in the context of familial relation and

[54] Proposed Rule at 49065.
[55] *Id.*
[56] *E.g.,* Proposed Rule at 49065-67.

confirming "biological sex," but offers little context for the actual fraud and security issues underlying the concern.

The rulemaking fails to provide adequate evidence of the widespread fraud, pointing to few government reports that reference proportionately small amounts of fraud. In the eighty-four page, three column Proposed Rule, USCIS only points to three reports that contain specific numbers and examples to substantiate its fraud claims: an Office of the Inspector General report discussing a pilot test of Rapid DNA Testing to verify parent-child relationships,[57] a document from seven years ago regarding numbers of unaccompanied minors being apprehended at the border,[58] and a House Judiciary Committee Report discussing a humanitarian parole in place program.[59] Of those data points provided by the reports, the most recent and relevant one to this rulemaking is the fraud related to verification of familial relationships. Between June 2019 and September 2021, DHS reported 3,516 instances of groups of people who were suspected of misrepresenting familial connections.[60] DHS tested the suspect individuals and found that only 8.5% of the suspected fraudsters actually misrepresented genetic relationships.[61] Requiring DNA tests to prove genetic

[57] OIG Report 22-27, *CBP Officials Implemented Rapid DNA Testing to Verify Claimed Parent-Child Relationships*, Off. Of Inspector Gen. Dep't of Homeland Sec. (Feb. 8, 2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-02/OIG-22-27-Feb22.pdf [hereinafter "OIG Report"].
[58] Press Release, Unaccompanied Alien Children and Family Units Are Flooding the Border Because of Catch and Release Loopholes, Dep't. of Homeland Sec., (Feb. 15, 2018), https://www.dhs.gov/archive/news/2018/02/15/unaccompanied-alien-children-and-family-units-are-flooding-border-because-catch-and.
[59] Interim Staff Report of the H. Comm. on Judiciary, 118th Cong., *The Biden-Harris Administration's CHNV Parole Program Two Years Later: A Fraud-Ridden, Unmitigated Disaster* (Nov. 20, 2024), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/2024-11-20%20The%20Biden%20Harris%20Administration%27s%20CHNV%20Parole%20Program%20Two%20Years%20Later%20-%20A%20Fraud-Ridden%2C%20Unmitigated%20Disaster.pdf. [Hereinafter "Judiciary Committee Report"].
[60] OIG Report, *supra* note 53 at 4.
[61] *Id.*

relationships potentially every time an individual applies for a benefit for a dependent or other family member is fundamentally disproportionate to the level of actual risk occurring.

Furthermore, much of the fraud statistics in the Congressional report cited by the Proposed Rule point to issues not with immigrants withholding information from USCIS, but in fact USCIS itself failing to flag individuals who admitted to being ineligible for the process.[62] For example, the report discusses USCIS approving applications for individuals who admitted that part of their reported income was derived from criminal activity.[63] This points to processing issues within USCIS, not individuals committing fraud and withholding information from USCIS.

USCIS's Proposed Rule also creates, without any statutory basis, a system for testing an individual's biological sex through DNA testing, stating that it would do so when biological sex would render an individual ineligible to receive a particular benefit. This continues the government's discriminatory treatment of transgender and other gender non-conforming individuals. It is unclear what benefits an individual would be ineligible for should their biological sex be different from what is on their application. For example, the Violence Against Women Act allows both women AND men to apply for benefits, including a green card.[64] There are no gender specifiers in the language for who is eligible. The only cited justification related to biological sex was one related to athletic competitions, citing the administration's Executive Order attempting to bar transgender individuals from competing in sports that don't align with their sex assigned at birth.[65] There is no actual benefit that an individual will be barred from simply because their sex assigned at birth does not align with their current gender presentation.

---

[62] Judiciary Committee Report, *supra* note 54 at 2-3.
[63] *Id.*
[64] NPRM at 49086.
[65] NPRM at 49079; Exec. Order 14201 Keeping Men Out of Women's Sports, 90 Fed. Reg. 9279 (Feb. 11, 2025).

It is hard to quantify the number of individuals currently in the U.S. immigration system. In fiscal year 2022, DHS reported about 2.4 million encounters with noncitizens at the southwest land border.[66] On average, around 800,000 individuals become naturalized citizens (i.e. ending the years-long process of lawful permanent residence and the application to become a citizen).[67] USCIS assumes in its cost analysis that around 880,000 individuals will provide DNA samples at least yearly to engage in continuous vetting.[68] To repeatedly collect the DNA of so many individuals yearly and process that information in a timely manner to approve or deny the benefits they are applying for would drastically increase the timeline and cost of the immigration system.

This rulemaking would violate the privacy of the hundreds of thousands of individuals year over year who claim genetic relationships with their family members to find a comparably small group of individuals actually committing fraud. Creating a system that automatically collects the DNA of potentially hundreds of thousands of individuals annually to prevent a fraud rate of 0.01% is overbroad and inconsistent with the FIPPs.

Requiring DNA tests would also extend the timeline individuals face when applying for benefits and changes in status. Immigrants already spend several months (or years) awaiting responses from USCIS[69] and can spend decades from the moment of entry to becoming a naturalized citizen.[70] Even though the system is known to be slow, individuals still show up by the hundreds of

---

[66] Sean Leong, *U.S. Naturalizations: 2020 Annual Flow Report*, Off. Of Immigration Stat. Office Dep't. of Homeland Sec. (Oct. 2021), https://ohss.dhs.gov/sites/default/files/2023-12/2021_1004_plcy_naturalizations_fy2020v2.pdf.

[67] 2022 Yearbook of Immigration Statistics, Off. Of Homeland Sec. Statistics, Dep't of Homeland Sec. (Nov. 2023), https://ohss.dhs.gov/sites/default/files/2024-03/2023_0818_plcy_yearbook_immigration_statistics_fy2022.pdf.

[68] Proposed Rule at 49110.

[69] *See, e.g.,* Alison Moodie, *Green Card Processing Times – FY 2025*, Boundless Immigration (Apr. 1, 2025), https://www.boundless.com/immigration-resources/average-green-card-wait-times.

[70] On average, individuals spent 7.5 years as lawful permanent residents before becoming naturalized. In most cases, individuals must be lawful permanent residents for at least 5 years before they are eligible to become naturalized citizens. These seven years do not include wait times to get visas nor the intial application for the lawful permanent resident status in the first place. *Naturalization Statistics*, U.S. Citizenship and Immigration

thousands every year, entering the system anew. By keeping people in the system longer, USCIS has a higher burden of individuals to track, data to keep organized, and parallel streams of work.

b. USCIS's Proposed Rule makes the immigration system more onerous and the agency fails to take into account the privacy and security costs of mass biometric collection.

The increased collection of biometrics also creates a significant burden on immigrants engaging in the process, both in needing to appear more often in person to submit biometric information and/or requiring the purchase of a smartphone that supports the apps that USCIS would require for remote biometric identification. This is further compounded by the fact that USCIS is limiting the ability to reschedule such appointments to highly extraordinary circumstances. By both requiring more of these appointments and leaving little wiggle room for scheduling, a person is far more likely to get their application falsely flagged and/or rejected for circumstances out of their control. For example, just a DNA test to verify familial relationships could cost between $400 and $800 per individual.[71] This cost is prohibitive and will mean vulnerable populations without money would not be able to complete the process and would be denied access to benefits they would otherwise be eligible for.

The increased collection of biometrics also puts a tremendous burden on applicants to make an impossible calculation regarding the privacy risks and costs – a cost which USCIS fails to consider. This includes the fact that USCIS plans to expand the collection of immutable biometric information and retain that information for decades at a time. There is no comprehensive regulation of biometric data that would provide the transparency, oversight, and accountability necessary to protect the privacy, civil liberties, and civil rights of the people providing the data. Applicants have good reason to be wary of handing over such sensitive data. The current administration has shown a

Services, (last updated Jan. 24, 2025), https://www.uscis.gov/citizenship-resource-center/naturalization-statistics.

[71] Proposed Rule at 49103.

willingness to use data collected by one agency for a specific purpose for the unrelated purposes of other agencies.[72]

USCIS's Proposed Rule also increases the security costs associated with the vast volume of biometric data it proposes to collect in ways the agency fails to take into account. In its cost analysis, USCIS does not account for the cybersecurity protections and systems it would need to implement to safeguard this highly sensitive data. Nor does USCIS consider the time it takes for field agents to learn how to properly collect biometric data such as DNA, the time it takes for the equipment to run its verification, and the time it takes to resolve falsely flagged individuals with follow up appointments.

Perhaps most egregiously with respect to the security risks, USCIS fails to properly consider the likelihood that the biometric data the agency collects will be breached at some point. Whether because of lax security, the exploitation of software vulnerabilities, or a programming error, DHS has consistently suffered data breaches that have exposed millions of people's sensitive data—including biometric data. In 2019, a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from CBP's Biometric Entry/Exit pilot.[73] When Perceptics, LLC was subsequently hacked, outside agents had access to those 184,000 images and an additional 105,000 license plate images.[74] With respect to this breach, the Office of the Inspector General concluded that CBP "[d]id not adequately fulfill its responsibilities for IT security."[75]

---

[72] *See, e.g.*, Kimberly Kindy and Amanda Seitz, *Trump administration gives personal data of immigrant Medicaid enrollees to deportation officials*, AP (Jun. 14, 2025), https://apnews.com/article/medicaid-deportation-immigrants-trump-4e0f979e4290a4d10a067da0acca8e22.
[73] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf .
[74] *Id.* at 8.
[75] *Id*.

More recently, DHS's Office of Intelligence and Analysis exposed sensitive information from multiple agencies for two months in 2023 because of a programming error that left the intelligence portal open to tens of thousands of unauthorized users.[76] The unauthorized users included government and private sector workers as well as foreign nationals.[77] Data breaches are common across the federal government and DHS is no exception, exposing the sensitive personal information of millions to exploitation and abuse. It follows that DHS and its subcomponents, as the FIPPs requires, should minimize the data the agency collects, particularly sensitive information like biometrics data. Consequently, USCIS should not expand its collection and use of biometrics without an extremely compelling reason and the security necessary to protect it. The agency has shown neither.

IV. Biometrics create intolerable privacy, civil rights, and civil liberties risks and should not be used as a form of identity management when other, less intrusive alternatives exist.

The overbroad collection of multiple biometric markers is not necessary. As mentioned above, biometrics are each distinct and highly sensitive categories of data to collect. They create substantial privacy, civil rights, and civil liberties dangers. This Proposed Rule would require the collection and use of highly sensitive data for routine and near constant verifications throughout the immigration process, which can often take over a decade.

To be able to safeguard such sensitive (and voluminous) amounts of data for such a long period of time from both other government officials querying it beyond its intended verification use and from bad actors hacking government databases is naïve and nearly impossible.

[76] Andy Greenberg, *A DHS Data Hub Exposed Sensitive Intel to Thousands of Unauthorized Users*, Wired (Sept. 16, 2025), https://www.wired.com/story/a-dhs-data-hub-exposed-sensitive-intel-to-thousands-of-unauthorized-users/.
[77] *Id*.

Rather than using official, legal documents for identity verification such as driver's license cards, state identification cards, passports, or the other myriad of legal documents in a person's possession that may identify them easily and securely, USCIS argues that biometrics is the only secure way to verify and manage identity. This is simply not the case! For example, for remote phone calls, an individual could use a voice obscuring technology to call centers where USCIS wants to implement voice recognition.

There are better ways to prevent fraud (to the extent it exists) than biometric verification, which create intolerable privacy risks. Instead of an identity marker tied to immutable and sensitive biometrics, USCIS could create a highly secure identity card. The government already creates higher security identification cards such as passports which include a picture and have embedded security characteristics that are hard to falsify.[78] Such a card could be further secured and would offer several benefits. It would not be tied to a person's immutable characteristics that would then be subject to countless verification checks with unreliable technology in less-than-ideal conditions. Instead, the card would act as a pre-certified identification marker that could easily be verified. Furthermore, a secure document would be harder to circumvent through AI spoofing technology.

This Proposed Rule would give DHS wide latitude to implement new surveillance technologies on vulnerable populations with little transparency and oversight. USCIS would alter existing forms from mentioning specific modalities of biometrics, such as fingerprint collection, to generally using the term "biometrics."[79] This generalization gives USCIS broad latitude to collect any manner of data from individuals who submit these forms instead of specific types of biometric data that would be fit for the specific purpose of collection. For example, facial recognition would

[78] *Next Generation Passport,* Travel.State.Gov (last updated Feb. 12, 2024), https://travel.state.gov/content/dam/passports/passport-images/NGP%20Infographic%20No%20TSG%20link.jpg.
[79] Proposed Rule at 49067.

not be a suitable tool to verify familial relationships in the same way that DNA tests could confirm or deny such relationships. For each purported reason of collection, USCIS must engage in the appropriate and legally mandated due diligence for each modality of biometric data collection to ensure that the technology is fit for purpose and is in line with the FIPPs. For example, privacy impact assessments and systems of records notices would have to be updated to include the new purpose of collection.

V. This Proposed Rule does not further USCIS's mission and puts privacy, civil rights, and civil liberties of specific vulnerable populations at risk.

Consistent with this Proposed Rule in general, the updates that target specific vulnerable populations fail to further the agency's mission. Specifically, USCIS proposes to use DNA to confirm biological sex and expand the collection of biometrics to minors under the age of 14. Both proposals lack the justification necessary to warrant its implementation.

a. The collection of DNA to confirm biological sex has no justification and is fueled by anti-transgender animus.

USCIS's proposal to vastly expand biometric data collection from anyone seeking or connected to an immigration benefit would cause particular and profound harm to intersex, transgender, and nonbinary people. The rule would allow USCIS to extract raw DNA and conduct DNA-based tests to "prove or disprove" a person's so-called "biological sex." This is an invasive and discriminatory practice built on an imprecise and undefined concept. For example, at least 1.7% (or 141,100,000 individuals worldwide) of people are intersex.[80] Their "biological sex" markers may be unconfirmed. For example, someone who has many of the phenotypical attributes of a "male" may in fact have XX chromosomes or hormone levels that may be associated with "female" sex markers. There have already been cases of individuals who have undergone discriminatory and

[80] Intersex People, United Nations Hum. Rts. Off. Of the High Comm'r. (last visited Jan. 2, 2026), https://www.ohchr.org/en/sexual-orientation-and-gender-identity/intersex-people (collecting publications from 2016-2023).

humiliating biological sex testing only to find out, well into adulthood, a very intimate and new facet of their body that is then disclosed to various unknown parties.

"Biological sex" is routinely misused to police and target intersex, transgender, and nonbinary people, and USCIS's proposal would codify that misuse into federal practice. Self-attestation and existing documentation already provide the information needed to administer immigration benefits. There is no legitimate policy reason to replace those longstanding methods with coercive genetic testing. Instead, the rule would give USCIS license to subject anyone it suspects of being intersex, transgender, or nonbinary to intrusive DNA testing - tests that could influence or even derail their ability to secure immigration benefits, remain with their families, or live safely in the United States due to a completely unnecessary factor.

The consequences would be immediate and harmful. Intersex, transgender, and nonbinary immigrants already face disproportionate scrutiny, violence, and barriers throughout the immigration system. This Proposed Rule would add yet another layer of risk, reinforcing stigma and creating strong disincentives to seek benefits for which individuals are legally eligible. By linking routine biometric collection to determinations of "biological sex," USCIS moves toward a genetic definition of identity that threatens everyone's bodily autonomy and self-determination - not just the communities most directly targeted. This provision should be removed from the proposed rule in its entirety.

b. USCIS fails to justify the expansion of collection of biometric data to minors under the age of 14.

USCIS does not justify why it needs to collect various biometrics from individuals under the age of 14. The Proposed Rule describes various specific instances where biometric identity verification may be "necessary," such as through deportation procedures of unaccompanied children. There is no reason that a secure identity card could not be made to follow the child through the

system instead of relying on biometrics that are notoriously unreliable for children.[81] They age and grow and their faces, fingerprints, voice, and other biometric markers change rapidly and unpredictably.[82] Instead, if there is proper documentation of children as they transit through various immigration centers, there should be no need for such unreliable technology for identity verification.

VI. The Proposed Rule exceeds USCIS's statutory authority.

USCIS claims it has authority to make all immigrants and U.S. citizens associated with any routine immigration benefit request submit intensely personal biometric information.[83] However, USCIS cannot point to any statute that authorizes collection of ocular images, voice prints, DNA, and facial recognition imagery in the context of routine immigration benefits. Rather, USCIS renames what it is authorized to collect for routine immigration benefits—fingerprints, photos, and signatures—into the catchall term of "biometrics" and then claims outsized authority to collect biometrics in general. That government agencies "have grouped together identifying features and actions, such as fingerprints, photographs, and signatures, under the broad term, biometrics" matters little.[84] The fundamental question remains whether USCIS's statutory authority grants them the ability to mandate biometric collection from a broad swathe of American society for routine immigration benefits. It does not.

a. USCIS cannot mandate biometric collection of ocular images, voice prints, DNA, and facial recognition imagery for routine immigration benefits.

USCIS points to a nebulous collection of statutes to assert broad authority to collect biometrics writ large for routine immigration benefits. But none of the statutes cited contain such a

---

[81] *See, e,g.,* Lindsey Barrett, *Ban Facial Recognition Technologies for Children—And for Everyone Else*, Boston Univ. J. of Sci. and Tech. L. 2 (last revised Nov. 12, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3660118#.
[82] *Id.*
[83] DHS' definition of benefit request is capacious to say the least. A benefit request includes "all requests processed by USCIS" including those that do not meet the definition of benefit requests under its own definition. Proposed Rule at 49063 n. 4.
[84] Proposed Rule at 49066.

delegation of power. 8 U.S.C. 1103(a)(1) gives the Secretary of Homeland Security general power to enforce provisions of the Immigration and Nationality Act (INA), but USCIS does not cite to any provision of INA that gives authority to collect biometrics for routine immigration benefits. At most, USCIS cites to provisions such as 8 U.S.C. 1357(b) and 8 U.S.C. 1225(d)(3) which allow the Secretary and immigration officers "to take and consider evidence."[85] But the "take and consider" clauses do nothing more than allow officers to collect documentary and testimonial evidence for immigration purposes. Any broader reading of those statutes exceeds both Congressional intent and plain language.

One of the earliest mentions of the "take and consider" clause was in 1891, when Congress first created the office of "superintendent of immigration" within the Department of Treasury.[86] Inspection officers and their assistants were given the power "to take and consider testimony touching the right" of any immigrant to enter the United States and were directed to record such testimony.[87] Subsequent revisions of the "take and consider" clause were codified in the 1917 Immigration Act where inspectors were authorized to "take and consider evidence" and, where it might be necessary, "make a written record of such evidence."[88]

In *Wong Yang Sung v. McGrath*, the Supreme Court considered whether deportation proceedings impermissibly comingled "the duties of prosecutor and judge."[89] When considering the "take and consider evidence" clause, the Court construed it as an investigatory function that allowed officers to take, record, and consider evidence "to enable the preparations of complaints for

[85] *Id.* at 49070.
[86] Act of Mar. 3, 1891, ch. 551, §7, 51 Stat. 1084, 1085 (1891).
[87] *Id.* at § 8.
[88] Immigration Act of Feb. 5, 1917, ch. 29, § 16, 39 Stat. 874, 886 (1917).
[89] 39 U.S. 33, 41 (1950).

prosecutive purposes."[90] There, too, the "take and consider" clause functioned to allow officers to take testimonial and documentary evidence.

DHS' own implementation of the statute shows the actual purpose of the "take and consider" clause is to collect documentary and testimonial evidence. DHS' model 287(g) MOU, for example, designates participating law enforcement officers with authority under INA § 287(b), 8 U.S.C. § 1357(b) "to complete required fingerprinting, photographing, and interviewing, as well as the preparation of affidavits and the taking of sworn statements for ICE supervisory review."[91] The "take and consider evidence" statutes do much less than what USCIS tries to claim: a carte blanche authority to demand any materials that it wants.

When USCIS does refer to specific statutes and regulations that authorize evidence collection to adjudicate routine immigration benefits, they consist entirely of evidence types such as fingerprinting and photographs. For example, the asylum requirements, codified under 8 U.S.C. 1158, authorize that the Attorney General "may require applicants to submit *fingerprints and a photograph* at such a time and in such manner to be determined by regulation by the Attorney General."[92] Nowhere is there any authorization to collect additional biometrics. The same is true for other routine benefits. For example, naturalization statutes authorize collection of "[t]hree identical photographs."[93] Registration obligations for those older than fourteen specifically authorize "fingerprinting."[94] None of these authorities include broad authority to collect biometrics beyond photographs, fingerprints, and signatures.

---

[90] *Id.* at 53.
[91] Dep't of Homeland Sec., Immigr. & Customs Enf't, *Memorandum of Agreement: 287(g) Task Force Model*, 2 (revised Aug. 19, 2025), https://www.ice.gov/doclib/about/offices/ero/287g/moaFillableTFM.pdf.
[92] 8 U.S.C. 1158(d)(1) (emphasis added).
[93] 8 U.S.C. §1444.
[94] 8 U.S.C. 1302(a).

When Congress has authorized DHS to collect additional types of biometrics, it has done so in explicit and narrow terms. Congress has granted DHS authority to collect biometrics in *specific* border crossing contexts.[95] Other references to biometrics collection exist, for example, for the regional center program which is a specific statutory scheme for individuals who "may provide capital to, or be directly or indirectly involved with, the ownership or administration" of a regional center, a new commercial enterprise, or other job creating entity.[96] The regional center program is a specific program with an accelerated timeline for lawful permanent resident status[97] and is entirely different from the routine immigration benefits that USCIS wishes to target for mandatory biometrics submission.

Other examples of permitted biometric data collection include the Kendall Frederick Citizenship Assistance Act, intended to streamline naturalization processes for non-U.S. Citizens in the United States Armed Forces. There, Congress authorized collection of "fingerprints and other biometric information for members of the Armed Forces."[98] Even then, as the Senate Judiciary Committee referred the bill out to the Senate to be voted on, Senator Leahy noted that:

> ...the language in this bill with respect to biometric information should in no way be misconstrued as authority for the administration to unilaterally expand the type of biometric information beyond what is currently required to obtain immigration benefits from the U.S. government. Federal immigration law is the province of the Congress, and Congress retains the sole power to determine the extent of rulemaking authority afforded to Federal immigration agencies. The involvement of Congress in these decisions is crucial to ensure that the procedures by which we admit or deny individuals entry to the United States take into account the interests of privacy, and are faithful to the welcoming traditions by which our nation has prospered. Only

[95] *See* 8 U.S.C. §1101(a)(6) (codifying requirements for "border crossing identification cards"); *see* 8 U.S.C. §1365b (requiring a biometric entry and exit data system after findings of the National Commission on Terrorist Attacks Upon the United States).
[96] 8 U.S.C. 1153(b)(5)(H)(iii).
[97] Holly Straut-Eppsteiner, Cong. Rsrch. Serv., IF13040, *In Focus: Overview of the EB-5 Immigrant Investor Program* (Jun. 23, 2025), https://www.congress.gov/crs-product/IF13040.
[98] Kendall Frederick Citizenship Act, §2, Pub. L. No. 110-251, 75 Stat. 2319 (2008) (codified at 8 U.S.C. 1440f).

> Congress can provide the deliberative, democratic process necessary to ensure that any future requirements are consistent with American values.[99]

But here, USCIS is doing precisely that: misconstruing its authority to unilaterally expand the type of biometric information required to obtain immigration benefits. USCIS alludes to a host of law enforcement statutes and requirements for background checks but never points to where these statutes authorize USCIS to collect broad biometrics data. Nor can it. Congress has never given it such authority.

Indeed, such broad authority to collect biometrics has been "subject of an 'earnest and profound debate' across the country...mak[ing] the oblique form of the claimed delegation all the more suspect."[100] Even when Congress tasked Customs and Border Protection to study biometric technology in the entry-exit system, it included explicit instructions that DHS could not "facilitate or expand the deployment of the biometric technologies, or otherwise collect, use or retain biometrics, not authorized by any provision of or amendment made by" the Intelligence Reform and Terrorism Prevention Act of 2004[101] or the Implementing Recommendations of the 9/11 Commission Act of 2007.[102] [103] DHS now attempts to grasp that authority outside Congress' deliberative, democratic process and grab the personal biometric data of millions of people with no clear authorization.

b. USCIS cannot mandate biometric data from U.S. citizens, nationals, and lawful permanent residents associated with routine immigration benefits.

USCIS purports to mandate biometric data from U.S. citizens, nationals, and Lawful Permanent Residents "to better ensure that it can comply with existing laws."[104] These laws include the Adam Walsh Child Protection and Safety Act of 2006 (AWA) and the International Marriage

[99] 154 CONG. REC. S1891 (daily ed. Mar. 11, 2008) (statement of Sen. Patrick Leahy).
[100] *Gonzalez v. Oregon,* 546 U.S. 243, 267-68 (2006).
[101] Public Law 108-458; 118 Stat. 3638.
[102] Public Law 110-53; 121 Stat. 266.
[103] 6 U.S.C. §1118(b).
[104] Proposed Rule at 49085.

Broker Regulation Act (IMBRA).[105] But, as detailed above, USCIS does not have the authority to collect information under its proposed expansive definition of biometrics. There is no mention of any collection of palm print, voice print, iris image, or DNA collection in either statute. USCIS claims authority far beyond what it has been granted.

Aside from those fatal flaws, USCIS' invocation of the AWA to create a biometric registry of Americans clearly distorts the purpose of the act. The AWA explicitly created and implemented a sex offender registry program to ensure compliance with its mandate to protect children.[106] The AWA imposes obligations on sex offenders as well as jurisdictions to report information.[107] This statutory scheme was carefully crafted to ensure "the civil liberties of Americans are not in jeopardy with this," as then-Senator Biden who sponsored the AWA put it.[108]

USCIS seems to believe that the existing sex offender registry is insufficient to meet USCIS' obligations because there *may* be crimes that fall outside of those that require individuals to have a protective order or be on the registry.[109] But USCIS does not state what those crimes may be. Nor does USCIS give a single indication that there have been any issues with AWA and IMBRA compliance that would be solved by increased biometric data collection. USCIS claims it needs additional biometrics to get access to the FBI's Identity History Summary Check, but such checks are accomplished via fingerprints.[110] Nonetheless, USCIS seeks to collect numerous biometrics far beyond what is currently permitted or necessary for such checks. Such a result is far beyond what

---

[105] *Id.*
[106] *See* 34 U.S.C. § 20903 (creating a tribal sex offender registry program); 34 U.S.C. § 20912 (creating a registry for "each jurisdiction"); 34 U.S.C. § 20921 (creating a national sex offender registry program).
[107] *See* 34 U.S.C. § 20914 (requiring certain information from offenders and jurisdictions for the registry).
[108] 152 CONG. REC. S8013 (daily ed. July 20, 2006) (statement of Sen. Joseph Biden).
[109] Proposed Rule at 49086.
[110] *See* FBI, *Identity History Summary Checks (Law Enforcement Requests)*, https://le.fbi.gov/informational-tools/identity-history-summary-checks (last visited Dec. 16, 2025).

Congress intended with the AWA and IMBRA and is clearly outside the bounds of USCIS' authority.

In fact, Congress has explicitly stated that DHS does *not* have the authority to subject U.S. citizens to mandatory biometrics collection. CBP instated opt-out protocols for its biometric exit-entry program for U.S. citizens after Senators Markey and Lee sent a letter to CBP regarding its biometric entry-exit program.[111] As the Senators noted, "while Congress has repeatedly voted to authorize biometric entry-exit scanning of foreign nationals, it has never authorized biometric exit scanning for U.S. citizens. In fact, Congress has pointedly neglected to authorize DHS to use the program on U.S. citizens for any purpose."[112] The House Committee on Homeland Security held two hearings which chastised DHS and CBP officials for their failure to ensure that Americans could opt-out of the biometric entry-exist program.[113] Nothing has changed since then. No bill has passed that contemplates giving DHS authority to mandate biometric data collection from Americans. Yet USCIS purports to claim that authority based on decades-old statutes intended for entirely different purposes.

Because USCIS does not have authority to mandate biometric data collection and its Proposed Rule far exceeds its statutory authority, it must rescind the rule.

VII. Conclusion

DHS's proposed rule to expand the collection and use of biometric modalities and information is ill-advised. DHS should immediately rescind the proposed rule and commit to only

---

[111] Letter from Sens. Edward J. Markey & Mike Lee to Kirstjen Nielson, Secretary of Homeland Sec. (Dec. 21, 2017), https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20.pdf

[112] *Id.* at 2.

[113] House Comm. on Homeland Sec., *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies* (July 10, 2019); House Comm. on Homeland Sec., *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies Part II* (Feb 6, 2020).

using biometrics where explicitly authorized by congress, ensure the FIPPs are appropriately considered for any proposed or current use of biometrics, and narrow the use of biometrics to the bare minimal needed to affect its mission. For further questions, please contact EPIC Senior Counsel Jeramie Scott at jscott@epic.org or EPIC Counsel Maria Villegas Bravo at villegasbravo@epic.org.

Respectfully Submitted,

Jeramie Scott
EPIC Senior Counsel and Director of EPIC's
Surveillance Oversight Program

Calli Schroeder
EPIC Senior Counsel

Maria Villegas Bravo
EPIC Counsel

Kabbas Azhar
EPIC EJW Fellow