epic.org

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

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

Sent via email to: DHSDeskOfficer@omb.eop.gov

Chad Wolf
Acting Secretary
U.S. Department of Homeland Security
301 7th Street, S.W.
Washington, D.C. 20528

September 30, 2020

Paul Ray
Acting Administrator
Office of Information and Regulatory Affairs Office of Management and Budget
725 17th Street, N.W.
Washington, D.C. 20503

Mr. Michael J. McDermott
Department of Homeland Security, U.S. Citizenship and Immigration Services
Security and Public Safety Division, Office of Policy and Strategy
20 Massachusetts Ave. NW
Washington, DC 20529-2240

Re: The Necessity of a 30-day or More Extension of Time to Submit Comments Regarding Notice of Proposed Rulemaking: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS Docket No. USCIS- 2019-0007, 85 FR 56338)

Dear Acting Secretary Wolf, Acting Administrator Ray, and Acting Division Chief McDermott,

The Electronic Privacy Information Center (EPIC) is a leading privacy and civil liberties organization that frequently comments on Department of Homeland Security's (DHS) biometric data policies and practices. EPIC is deeply concerned about authorizing DHS and ICE to collect new types of information, including DNA and voiceprints as well authorizing ICE to collect biometrics from a much broader section of the population. EPIC urges the Department of Homeland Security to provide the public at least 30 more days to comment on the proposed massive expansion of DHS's collection of biometric information.[1] The proposed rule will affect millions of individuals. 30 days is not enough time for the public to read and meaningfully respond to the 85-page notice.

Under the proposed rule DHS would increase the collection, storage, and analysis of biometric data by adding millions of individuals, including many U.S. citizens, to DHS's biometric databases. The core of the rule would require "any applicant, petitioner, sponsor, beneficiary, or individual filing or associated with a certain benefit or request, including U.S. citizens and without regard to age, must appear for biometrics collection unless DHS waives or exempts the

[1] EPIC joins over 100 civil society organizations in requesting an extension. Letter from Catholic Legal Immigration Network, Inc., et al., to Chad Wolf, Acting Secretary, Dep't of Homeland Sec. et al. (Sept. 16, 2020), https://www.americanimmigrationcouncil.org/sites/default/files/general_litigation/letter_requesting_60day_comment_period_on_proposed_rule_expanding_collection_of_biometrics.pdf.

requirement."[2] In addition, DHS proposes to eliminate age restrictions currently preventing children younger than 14 from certain biometric collections.[3] DHS further proposes a system of "continuous immigration vetting" for any non-citizen resident and certain citizens, resulting in years of biometric data collection for individual immigrants.[4] Sweeping far more individuals into DHS's biometric databases is a substantial privacy and civil liberties concern.

The proposed rule would also expand the types of biometric data DHS can collect. For the first time DHS would claim the authority to require DNA test results to prove familial relationships. DHS's expansive definition of biometrics would approve the collection of fingerprints, palm prints, photographs for facial recognition, signatures, voice prints, iris images, and DNA.[5] The collection of new types of biometric information and the expansion of its use requires careful consideration of threats to privacy. The public deserves a meaningful opportunity to engage in those considerations from the outset.

Along with expanding biometric data collection, DHS in the same rule proposes to alter baseline assumptions of good moral character for several classes of immigrants. DHS would, for the first time, collect biometric information from women fleeing domestic violence and children under 14.[6] The proposed rule would also raise the bar to qualify for visas for women seeking shelter from domestic violence under the Violence Against Women Act by increasing the required time of "good moral character" from 3 years to a lifetime.[7] The rule also eliminates the presumption of good moral character for VAWA self-petitioners under the age of 14, subjecting children to increased scrutiny.[8] These are not cosmetic changes which can be ratified with a 30-day comment period but substantial changes to the process of determining immigration benefits and the rights of particularly vulnerable individuals.

The proposed collection is a major threat to individual privacy. DHS and its subcomponents have not demonstrated that they can adequately safeguard the biometric data the Department currently possesses. The Office of Inspector General at DHS recently found that in 2019 Customs and Border Protection failed to implement adequate security practices to prevent a data breach at a CBP subcontractor which exposed over 180,000 traveler images.[9] Expanding DHS's collection of biometrics, including incorporating new forms of data like DNA, poses substantial privacy risks.

DHS has not provided the public with enough time to respond to a rule which would re-work data collection and re-shape eligibility for immigration benefits for a large class of individuals. The proposed changes are a matter of public concern for many Americans for a variety of reasons: privacy, eligibility for immigration benefits, surveillance and more. EPIC urges DHS to allow the

[2]85 F.R. 56340.

[3] *Id.*

[4] *Id.*

[5] 85 F.R. 56341.

[6] 85 F.R. 56342.

[7] *Id.*

[8] *Id.*

[9] Joseph Cuffari, Ph. D, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Office of Inspector General (Sept. 21, 2020) https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

public sufficient time for a careful analysis and detailed comments on a major rulemaking which will affect the rights and privacy of millions. An extension of at least 30 days is warranted.

Sincerely,

Jeramie Scott
Senior Counsel
Electronic Privacy Information Center

Jake Wiener
Kennedy Fellow in Domestic Surveillance
Electronic Privacy Information Center