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

Office of Information and Regulatory Affairs,
Office of Management and Budget,
725 17th Street NW, Washington, DC 20503;
Attention: Desk Officer, U.S. Citizenship and Immigration Services, DHS

Collection and Use of Biometrics by U.S. Citizenship and Immigration Services
[CIS No. 2644–19 USCIS Docket No. USCIS– 2019–0007] RIN 1615–AC14

Our organization, the Immigrant Law Center of Minnesota, submits this comment urging the Department of Homeland Security (DHS) to withdraw this proposed rule in its entirety.

The Immigrant Law Center of Minnesota ("ILCM") enhances opportunities for immigrants and refugees through legal representation for low-income individuals, and through education and advocacy with diverse communities. ILCM serves immigrants and refugees residing in the state of Minnesota who earn less than 187.5 percent of federal poverty guidelines. In 2019, ILCM served clients coming from 115 countries, with 36 percent of ILCM cases originating from Mexico, 21 percent from countries in Central and South America, 20 percent from countries in Asia, 20 percent from countries in Africa, and the remainder from countries in Europe, Oceania, and from Canada.

ILCM provides a wide range of legal services to low-income immigrants and refugees, including representation of families seeking reunification, of immigrants applying for naturalization, and of refugees and asylum seekers and their families, and of unaccompanied children seeking Special Immigrant Juvenile Status.

Because this regulation covers so many topics, we are not able to comment on every proposed change. The fact that we have not discussed a particular change to the law in no way means that we agree with it—we oppose this proposed rule in its entirety and call upon the agencies to withdraw it.

I. We object to the shortened comment period for the Notice of Proposed Rulemaking (NPRM).

Especially during this time of COVID-19, our resources, and the resources of other legal representatives of immigrants, are stretched to the breaking point. We have less access to our offices and to the resources needed to comment on this NPRM. We have not had full access to our offices since early March.

This NPRM is more than 325 pages in length. The changes made by the rule would apply to over six million people at a cost of nearly $300 million each year, require the collection of data on millions of American citizens and immigrants, and represent one of the most significant changes to the legal immigration process in generations. In order to adequately prepare comments on this long and complex proposal, we need more than 30 days.

Two Executive Orders (EO 12866 and EO 12563) state that the normal period for public comment on proposed regulations should be *at least* 60 days. In the case of an extremely complex and lengthy NPRM such as this one, an even longer comment period is needed. Moreover, with the nation still in the midst of the COVID-19 pandemic, which affects government and members of the public, including the staff of ILCM, the 30-day comment period is intolerably short and prevents full and detailed response to the NPRM.
We urge that this proposed rule be withdrawn, based on procedural considerations alone. If the government wishes to issue this rule, it should comply with the customary and necessary 60-day comment period.

II. The proposed rule endangers U.S. citizens and immigrants alike.

The mass surveillance proposed by this rule is wholly unjustified. There is no showing that current vetting processes and information collection are inadequate. There is no showing of need, merely the assertion that "DHS has decided" that additional biometric collection is needed.

DHS proposes maintaining an extensive database of biometric data—including fingerprint, palm print, facial recognition, photographic, voice print, iris image, and DNA evidence—on any citizen or non-citizen who applies for an immigration benefit or is associated with an application for such a benefit.

DHS also proposes sharing all of this data with law enforcement, which further expands the possibilities of abuse of information or outright data hacking and theft. There is no way to guarantee the security of thousands of law enforcement organizations' storage and use of biometric data shared with them by DHS. DHS has neither the capacity nor the authority to monitor these law enforcement organizations' data security protocols.

For years, local law enforcement organizations have maintained inaccurate gang databases that have been used to target immigrant youth. One example is the California's CalGang database. A 2016 audit by the California State Auditor found inaccurate information, inadequate oversight, and use of the law enforcement database for employment and military-related screenings. The problems were not remedied after this report, but continue into 2020, when the Los Angeles Police Department withdrew from the database because of inaccurate and false information contained in it and the California Attorney General revoked police access to much of the information contained in it. Similar abuses have been found in law enforcement databases in other cities, such as Chicago and New York.

In addition to sharing information with U.S. law enforcement agencies, DHS may have shared information on individuals with government agencies in their home countries. Pro Publica reported on a "fusion center" that involves collaboration between U.S. immigration authorities

and the notoriously corrupt and abusive Salvadoran police, as well as expansion of that collaboration to Honduras, Guatemala, and Mexico.

This regulation proposes collection and sharing of a vastly increased amount of biometric data, which will exponentially increase the potential for errors in and abuse of that information.

Apart from the significant dangers of sharing biometric information with law enforcement organizations, the maintenance of even a DHS database opens the door to hacking and identity theft. DHS in the past has been unable to protect the personal data of its employees. Data breaches at major corporations with seemingly endless resources are an everyday occurrence. There is no reasonable way the government could protect or should be trusted with this extensive amount of personal data.

Biometric data on immigrants maintained by DHS has already been hacked. A September 23, 2020 report by the DHS Inspector General's office found that a database of 184,000 facial recognition images collected by Customs and Border Protection in Texas had been hacked. Subsequently, at least 19 of the images were posted on the dark web. The expansion of biometric collection geometrically increases the danger of hacking and identity theft.

III. The proposed rule is fiscally irresponsible.

The expansion, which would apply to millions of people, would be extremely costly to the government in infrastructure and other resources. U.S. Citizenship and Immigration Services (USCIS) has recently declared it is nearly bankrupt. To simultaneously propose this type of expansion for no tangible reason is clearly fiscally irresponsible.

DHS is unable to adequately process the documents and fingerprints that it already collects. Every year the backlog of benefit applications grows longer. At the end of FY2018, USCIS reported a backlog of 2.4 million cases. How much additional time will be needed to process the far more complex information provided by a combination of fingerprint, palm print, facial recognition, photographic, voice print, iris image, and DNA evidence?

Not only does the proposed regulation ask for more types of information, but it also demands more frequent collection of biometric information from more people. This regulation creates a presumption of collection of biometric information from "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," unless a specific waiver decision is made. According to the NPRM, "2.17 million new biometrics submissions will be collected annually, and the resulting biometrics submitting population will increase from 3.90 million currently to 6.07 million."

This will exponentially increase both processing time and cost. Procedures are in place to process and store fingerprints and photographs. For each new type of biometric—palm prints, facial recognition, voice prints, iris images, and DNA evidence—new kinds of processing and storage will need to be implemented. That will mean creation of new infrastructure and then maintenance and storage of data for an indefinite future, or in perpetuity. How much will this

cost? The NPRM says: "DHS does not know … the costs of expanding biometrics collection to the government in terms of assets and equipment."

While the cost to USCIS will be immense, the cost to applicants in time and money will also escalate. DHS estimates that 1.63 million more people will be required to pay biometrics fees each year than under the current system. More than two million additional people will be required to appear for biometrics appointments each year. That will require time and travel costs for applicants, imposing particular hardships on those who live in rural areas or sites distant from biometric collection points.

IV. The proposed rule would do grave harm to vulnerable populations:

The proposal would harm all immigrants and many U.S. citizens, subjecting immigrants and them to extensive and ongoing collection of their DNA, voices, iris and face scans, and more.

Asylum seekers fleeing oppressive governments and survivors of abuse could be deeply traumatized by this collection and extreme surveillance. In the event of a data breach, lives would be at risk. The NPRM contemplates information sharing with the governments of immigrants' home countries, the very governments whose persecution is the reason for asylum seekers' flight to the United States. If the danger of this information sharing does not appear self-evident, recall the case of Orlando Letelier, assassinated inside the United States in 1976 by agents of the repressive government that he fled. More recent cases of repressive governments pursuing political opponents outside their own borders include the assassination of Jamal Khashoggi in Turkey and the attempted murder of Sergei Skripal in England.

Changes to determination of good moral character for VAWA and T visas also pose problems. Instead of letters from law enforcement officials who know the circumstances of their cases, the NPRM will substitute DNA collection and background checks. These applicants are particularly likely to have incurred baseless criminal charges directly associated with the abuse and exploitation they have suffered, and background checks will reveal only criminal charges and not the crucial background and context.

Missing a biometrics appointment could result in termination of status, multiplying opportunities for termination of status. Given the well-documented failures of notice in the ICE Notice to Appear process, adding one more mandatory appointment to the process increases the risk of systemic failure. This risk is heightened by ongoing cuts in service by the U.S. Postal Service, which may result in failure of forwarding and late delivery of notices.

The elimination of the existing presumption of good moral character for VAWA self-petitioners and T-visa applicants who are under 14 years of age targets one more vulnerable group. There is simply no good reason to remove this presumption of good moral character.

V. The proposed rule undermines U.S. democracy and principles.

This rule would expand surveillance and data collection on immigrants and U.S. citizens in a manner consistent with police state practices. It would eviscerate rights to privacy, enshrined in

our democracy. Bureaucratic errors and mismanagement with such a massive amount of data could lead to the separation of families, unjust detention, and more. As the use of technology expands across our country and the world, we should proceed responsibly and ensure that human rights and civil liberties are prioritized. This proposed rule fails to do that and must be withdrawn.

The Fourth Amendment protects against unreasonable search and seizure. The massive collection of highly personal data proposed in this NPRM constitutes a warrantless invasion of privacy. By way of justification, DHS cites various provisions in U.S. immigration law that allow collection of fingerprints and photographs and then conflates these with anti-terrorism provisions that provide for collection of biometric evidence.

The specific authorizations for collection of fingerprints and photographs does not translate to a blanket authorization of collection of any biometric data desired by DHS. Immigration statutes contain no such authorization.

No statute authorizes collection and maintenance of a databank of fingerprints, palm prints, voice prints, facial recognition data, iris images, and DNA evidence on more than 6 million immigrants and U.S. citizens annually. No statute authorizes sharing this data with U.S. and foreign law enforcement organizations. Such a massive change to current practice and to practice specifically authorized by immigration statutes must be approved by Congress, not implemented by executive fiat.