



Submitted online via regulations.gov

October 13, 2020

Samantha Deshommes
Chief, Regulatory Coordination Division
Office of Policy and Strategy
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
20 Massachusetts Avenue, NW
Washington, D.C. 20529-2140

Re: Docket ID number USCIS-2019-0007-0001; Collection and Use of Biometrics by U.S. Citizenship and Immigration Services

Dear Ms. Deshommes,

The Catholic Legal Immigration Network, Inc. (CLINIC)¹ respectfully submits the following comment in strong opposition to the Department of Homeland Security's (DHS) Notice of Proposed Rule Making (NPRM) published in the Federal Register on September 11, 2020. If implemented, the proposed rule would have devastating ramifications on the lives of millions of immigrants and their U.S. citizen and lawful permanent resident relatives. The proposed rule would dramatically expand government surveillance over immigrants—even children—and the U.S. citizens sponsoring immigration cases, collecting DNA, voice prints, iris and face scans as well other personal characteristics to be stored in government databases, potentially forever. It would authorize and facilitate the mass collection and storage of all manner of biometric information into a new database described by experts as “the largest database of biometric and biographic data on citizens and foreigners in the United States.” We urge DHS to withdraw the proposed rule in its entirety because it would authorize invasive data collection, storage, and sharing far beyond any legitimate justification connected to DHS's purpose.

Embracing the Gospel value of welcoming the stranger, CLINIC has promoted the dignity and protected the rights of immigrants in partnership with a dedicated network of Catholic and community legal immigration programs since its founding in 1988. CLINIC's network, originally comprised 17 programs, has now increased to close to 400 diocesan and community-based programs in 48 states and the District of Columbia. CLINIC is the largest nationwide network of nonprofit immigration programs. Through its affiliates, CLINIC advocates for the just and humane treatment of noncitizens through direct representation, pro bono referrals, and

¹ Benjamin L. Apt, Defending Vulnerable Populations (DVP) Program Consulting Attorney, Jill Marie Bussey, Director of Advocacy, Michelle N. Mendez, DVP Director, Miguel A. Naranjo, Director of Religious Immigrant Services, Rebecca Scholtz, DVP Senior Attorney, Susan Schreiber, Training and Legal Support Managing Attorney, Karen Sullivan, Federal Advocacy and Liaison Attorney, and Viviana Westbrook, State and Local Advocacy Attorney, authored these comments.

engagement with policy makers. CLINIC also provides direct representation and *pro bono* referrals through several projects: 1) the Board of Immigration Appeals (BIA) Pro Bono Project, 2) the Formerly Separated Families Project, 3) the Remote Motions to Reopen Project, and 4) Religious Immigrant Services. Through our work, CLINIC acknowledges the inherent dignity and value of all people. This proposed rule would impact nearly all of CLINIC’s clients, including religious workers, in addition to affiliates across the country, our affiliates’ clients, and the U.S. citizen and permanent resident family members of these clients. Immigrants and refugees would see their privacy rights eroded and face many more roadblocks that would prevent USCIS from approving their cases, families from reuniting, and refugees from receiving protection.

Throughout the Bible, migration emerges as an important theme that often signifies a turning point in the life of God’s people—from the migration of Abraham from his homeland of Ur to the promised land of Canaan; to the delivery of the Hebrew people out of slavery in Egypt by Moses; and the flight of the Holy Family under threat of persecution by Herod.² Catholic social teaching on migration, which is itself an outgrowth of both the Church’s ongoing engagement with Scripture and with the “signs of the times” of a particular period, provides a framework to understand how to engage the migration question in a particular situation. One of the key foundations out of which this teaching has emerged is in papal teaching.

Papal teaching recognizes the plight of refugees and asylum seekers who are compelled to leave their homeland because of political, religious, or other forms of persecution. In *Rerum Novarum*, Pope Leo XIII emphasized the fact that “no one would exchange his country for a foreign land if his own afforded him the means of living a decent and happy life.”³ If conditions enable individuals to build a satisfying life, they most likely will remain in their homeland and, if they leave, it is more likely by choice than by necessity. The corollary to this emphasis consists in ensuring that the conditions of a given country do not give rise to situations of forced migration. It is thus critical that we seek to offset and alleviate the root causes that compel people to migrate. In his encyclical letter *Sollicitudo Rei Socialis*, Saint Pope John Paul II refers to the world’s refugee crisis as “the festering of a wound.”⁴ Pope Benedict reminds us that “every state has the right to regulate migration and to enact policies dictated by the general requirements of the common good,” but every state must always do so “while safeguarding respect for the dignity of each human person.”⁵ Similarly, since the beginning of his pontificate, Pope Francis has recognized the dire circumstances confronting refugees and asylees as being of particular concern. Making a bold statement by taking his first papal trip outside Rome to Lampedusa, Italy, the Holy Father decried the “globalization of indifference” and the “throwaway culture”

² James Martin, S.J., *Were Jesus, Mary and Joseph refugees? Yes*. AMERICAN THE JESUIT REVIEW, <https://www.americamagazine.org/faith/2017/12/27/were-jesus-mary-and-joseph-refugees-yes>.

³ Pope John XIII, *Rerum Novarum*, THE HOLY SEE, May 15, 1891, #47, www.vatican.va/content/leo-xiii/en/encyclicals/documents/hf_1-xiii_enc_15051891_rerum-novarum.html.

⁴ Saint Pope John Paul II, *Sollicitudo Rei Socialis*, THE HOLY SEE, #24, www.vatican.va/content/john-paul-ii/en/encyclicals/documents/hf_jp-ii_enc_30121987_sollicitudo-rei-socialis.html.

⁵ Pope Benedict XVI, *2013 World Day of Migrants and Refugees Message*, THE HOLY SEE, (Oct. 12, 2012), www.vatican.va/content/benedict-xvi/en/messages/migration/documents/hf_ben-xvi_mes_20121012_world-migrants-day.html.

that disregards those fleeing persecution in order to seek a better life.⁶ It is, in this view, unacceptable for those of us in the developed world to disregard their suffering or to disregard their plights so that we might more easily live lives of comfort. Instead, the Holy Father has repeatedly highlighted our obligation as Catholics to nurture and support policies that will protect the human dignity of migrants, promote the stability of migrant families, and assist in their integration following their arrival.⁷ Indeed, Papal teaching instructs us to understand the plight of refugees and asylum seekers and recognize the persecution they may have endured; but Papal teaching also warns us against becoming a country from which people want to migrate.

“The family, a natural society, exists prior to the State or any other community, and possesses inherent rights which are inalienable.”⁸ Families and natural society comprise individual people. For this reason, respect for the family and natural society is impossible without first recognizing the inherent value of each individual person and respecting their individual freedoms, including the freedom of privacy. CLINIC condemns this proposed rule because it would violate the privacy rights of immigrants and refugees, and send yet another shameful message to the most vulnerable among us that the United States no longer recognizes their God-given dignity. Privacy is essential to the common good of a free society. Privacy rights convey government’s respect for its residents, instills trust in democratic institutions, and nurtures the creation of families. Privacy violations and policies that treat newcomers differently endanger immigrants, refugees, and, eventually, all U.S. citizens.

I. DHS HAS FAILED TO FOLLOW THE NPRM PROCESS AS REQUIRED BY THE ADMINISTRATIVE PROCEDURE ACT

As a general matter, CLINIC urges DHS to withdraw the proposed rule in its entirety because of deficiencies in the procedure through which the agency has promulgated this proposed rule and the problematic context of in which the agency has chosen to introduce this rule. Concerns regarding the length of the comment period, burden on the public, the consultation process, and the impact on case processing backlogs and budget shortfalls are described below.

a. DHS Has Not Afforded the Public a Meaningful Opportunity to Comment.

As a preliminary matter, DHS has not allowed the public sufficient opportunity to comment on this rule. The rule, nearly 90 pages in length, dramatically expands who will be subjected to biometrics collection, how long and how frequently the government could demand their information, and what type of information the government can collect about them.

Typically, the administration should allow a comment period of *at least* 60 days following publication of the proposed rulemaking to provide the public a meaningful opportunity to

⁶ Pope Francis, Homily during his visit at Lampedusa, THE HOLY SEE, (July 8, 2013), www.vatican.va/content/francesco/en/homilies/2013/documents/papa-francesco_20130708_omelia-lampedusa.html.

⁷ See, e.g., Pope Francis, *2018 World Day of Migrants and Refugees Message*, THE HOLY SEE, (Jan. 14, 2018), http://w2.vatican.va/content/francesco/en/messages/migration/documents/papa-francesco_20170815_world-migrants-day-2018.html.

⁸ *Charter of the Rights of the Family*, THE HOLY SEE, (Oct. 22, 1983), www.vatican.va/roman_curia/pontifical_councils/family/documents/rc_pc_family_doc_19831022_family-rights_en.html.

comment.⁹ The Administrative Procedure Act (APA) § 553 requires that “interested persons” from the public have “an opportunity to participate in the rule making.” In general, the agencies, must afford “interested persons a reasonable and meaningful opportunity to participate in the rulemaking process.”¹⁰ Courts have found that for agencies to comply with this participation requirement the comment period must be “adequate” to provide a “meaningful opportunity”¹¹ for public participation. DHS acknowledges that this rule is a “significant regulatory action” under section 30(f) of Executive Order 12866. Given the importance of the public’s participation in the rule-making process, Executive Order 12866 specifies that “in most cases [rulemaking] should include a comment period of not less than 60 days.”¹² Executive Order 13563 explicitly states, “To the extent feasible and permitted by law, each agency shall afford the public a meaningful opportunity to comment through the Internet on any proposed regulation, with a comment period that should **generally be at least 60 days.**”¹³

Here, despite the breadth and complexity of this proposed rule, DHS has afforded the public only 30 days to comment. There is simply no justification for rushing through a rule of this scope and magnitude, which, as DHS itself notes, would power biometric data collection for at least six million people annually and will cost taxpayers hundreds of millions of dollars. Artificially limiting the time period for comment is particularly unfair at this moment, given that members of the public are grappling with the many challenges of managing work and life during a global pandemic. Yet not only has DHS imposed an abnormally short deadline without any justification for doing so, it has also, to date, failed to respond to a request for extension of the deadline signed by over 100 organizations.¹⁴

Furthermore, the proposed rule is incomplete: it lacks information essential to affording the public a meaningful opportunity to comment. It fails to provide concrete data about the biometric information DHS currently collects and—other than conclusory statements about the reliability of documentary versus biometric information—does not explain why that information is insufficient to meet DHS’s stated objectives of identity verification and criminal and national security checks. Moreover, the proposed rule also fails to describe how the massive amounts of new data it plans to collect will be stored and shared, even though this is critical to understanding the rule’s ramifications. For example, the proposed rule mentions in a cursory footnote that DHS’s IDENT (Automated Biometric Identification System) database will be replaced by the Homeland Advanced Recognition Technology (HART) database and says that “DHS will use the term ‘IDENT’ in this rule to refer to both the current and successor systems.” Yet these two

⁹ See, e.g., EXECUTIVE ORDER 12866 (Oct. 4, 1993) (requiring that the public generally be given 60 days to comment on a proposed rule); EXECUTIVE ORDER 13563 (Jan. 18, 2011) (to provide the public an opportunity to participate in the regulatory process, comment period shall be at least 60 days).

¹⁰ *Forester v. CPSC*, 559 F.2d 774, 787 (D.C. Cir. 1977).

¹¹ *N.C. Growers’ Ass’n v. UFW*, 702 F.3d 755, 770 (4th Cir. 2012).

¹² See EXEC. ORDER No. 12866 – Regulatory Planning and Review, § 6(a), 58 FED. REG. 51735 (Oct. 4, 1993).

¹³ See EXEC. ORDER No. 13563 – Improving Regulation and Regulatory Review, 76 FED. REG. g. 3821 (Jan. 18, 2011) (emphasis added).

¹⁴ Letter from 104 non-governmental organizations to Chad Wolf, Acting Secretary, U.S. Department of Homeland Security and Paul Ray, Acting Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, (Sept. 16, 2020), <https://cliniclegal.org/resources/federal-administrative-advocacy/more-100-organizations-join-urge-dhs-provide-60-day>.

databases are hardly interchangeable: HART is cloud-based and will reportedly¹⁵ include a vast array of capabilities that IDENT doesn't have, including broadened-out data sharing agreements, without all the new aspects of HART having undergone a full privacy impact assessment.¹⁶ By failing to provide even the barest amount of transparency about where the massive amounts of data collected under this rule will be stored, let alone how it will be shared, the rule fails to provide necessary transparency about its potential ramifications.

DHS has failed to provide the public a meaningful opportunity to comment on its far-reaching impacts and therefore should rescind this rule. Notwithstanding CLINIC's objections to the limited time and information provided, CLINIC submits this comment to register our concerns about the grave consequences of the proposed rule.

b. The Proposed Rule Would Needlessly and Excessively Burden the Public.

The proposed rule would produce significant difficulties for millions of people. DHS proposes to become the nation's clearinghouse on a vast amount of personal biological information. Its program would apply to every arriving immigrant, including children, and would extend to a large number of U.S. citizens. Yet DHS neglects to offer a solid justification for the changes. This nonchalance toward substantiating a need for revisions to the definition of biometrics launches the rule into conflict with the APA. The APA prohibits agency actions that are "arbitrary, capricious, an abuse of discretion" as well as "unsupported by substantial evidence." This consideration must be addressed in the course of creating a rule. Yet over and over, the proposed rule makes assertions in place of reasons.

The proposed rule lacks a substantial defense for the biometric enhancements it seeks while also failing to address a fundamental question facing any proposed rule: what is the balance of public burden versus public benefit that it would produce? The public burden of this rule is glaring. It demands that U.S. citizens and immigrants surrender their most personal biological information to DHS. "Burden," for the purposes of regulatory analysis, is not limited to monetary cost.¹⁷ If the state demanded that all U.S. citizens appear outside every morning for an hour of calisthenics, the cost in dollars to the public would be difficult to calculate. But the intrusion into personal lives is sizable. Even if the proposed rule is meant to improve the public welfare, it still needs a logical account for how the benefit outweighs the burden.

Various federal agencies have fallen victim to data breaches. This risk is another public burden. Some of these events have received public attention,¹⁸ while others are little known outside of

¹⁵ Jennifer Lynch, "HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' 'Non-Obvious Relationships,'" www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

¹⁶ A privacy impact assessment is conducted to identify and mitigate privacy risks associated with DHS programs. For more on what privacy impact assessments are and when they are conducted. See *Privacy Impact Assessments*, www.dhs.gov/privacy-impact-assessments.

¹⁷ 44 USC Sec. 3502(2) (defining "burden" as "time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency . . .").

¹⁸ OPM, *What Happened*, Cybersecurity Incidents, Cybersecurity Resource Center, www.opm.gov/cybersecurity/cybersecurity-incidents/; Josh Fruhlinger, *The OPM hack explained: Bad security practices meet China's Captain*

the particular agencies. The errors resulted from a mixture of the agencies' carelessness or unsophistication and the advanced abilities of hackers. Hacking will continue to be a problem as long as the government routinely relies on a potpourri of outside contractors to handle its data.

For that matter, DHS does not indicate that it will periodically purge the data collection. To the contrary, the data will not only be preserved indefinitely, but DHS will readily share the DNA and other biometrics data with other federal law enforcement agencies. The rule's justifications for its policy are tortured and insufficient. It proposes to reap data without restraint and with the most open-ended of justifications.

Under the rule, DHS would compel an enormous swath of people to submit a plentitude of their biological information on the basis of a nebulous declaration that the agency will shield the public from identity theft (although the rule does not suggest how commonly this occurs, nor who commits it). One of the most disturbing elements of the rule is that DHS would submit immigrant children, regardless of age, to DNA collection. The rule tries to justify why children must surrender their genetic data as serving to secure them from identity theft and human trafficking. Rather than targeting perpetrators, the new biometrics regime would burden the potential victims, as described below.

c. DHS Failed to Engage in Proper Consultations on the Rule.

Given the practical consequences of the proposed changes for government at all levels, as well as individuals and their families, the proposed rule should have undergone a risk assessment and consultation process commensurate to the complexities associated with its implementation, including a federalism assessment.

Critically, the rule justification states that the regulation "will not have substantial effect on the States, on the relationship between the national Government and the States, or on the distribution of power and responsibilities among the various levels of government" and therefore does not warrant a federalism assessment.¹⁹ Yet, the HART database in which the information would be stored allows international, federal, state and local data sharing. The use of data at the state level is governed by state law and some functions, such as familial searching, are conducted and regulated only at the state level. Thus, legislation around the protection and sharing of data at the state level is highly relevant to this rule yet the NPRM does not discuss any consultation between DHS state lawmakers.

d. DHS Did Not Sufficiently Consider or Address the Case Adjudication Backlogs or the USCIS Budget Crisis.

DHS proposes to expand dramatically the types of biometrics collected, the population from whom they collect biometrics, and the frequency and duration of surveillance, but does not acknowledge the current backlogs in case adjudication at USCIS and its Asylum Office, or the current financial crisis at USCIS.

America, CSO (Feb. 12, 2020), www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

¹⁹ 85 FED. REG. at 56390.

The NPRM does not sufficiently analyze how these proposed changes would impact the significant and growing case processing backlogs, the lengthy and growing processing times for adjudication, and inefficiencies in customer service. Since 2010, USCIS' case adjudication backlog has increased by more than 6,000 percent,²⁰ the overall average case processing time had increased 91 percent between 2014 and 2018,²¹ and USCIS has removed language from its resources that stated any commitment to customer service.²² As of July 31, 2020, USCIS had 370,948 asylum applications pending final adjudication.²³ As CLINIC testified at a congressional hearing on delays at the agency, USCIS' adjudication backlogs are a self-inflicted problem resulting from poor policy and organizational choices that cause it to fail to meet the basic expectations of expedient and efficient adjudication of immigration benefits.²⁴ In addition to its self-inflicted inefficiencies, the COVID-19 pandemic has caused additional delays that have increased the backlogs.²⁵ This NPRM, like others before it, will cause significant delays in adjudication without sufficiently analyzing the extent of those delays, their impact on immigrants and their families, their impact on immigration legal services providers, or analysis of alternatives that would not impact adjudication times.

The NPRM does not sufficiently analyze the financial costs of the proposed changes given the context of USCIS's massive projected budget shortfall and ongoing financial instability. USCIS, which is funded almost entirely by application fees, predicted a budget shortfall of \$1.2 billion in November of 2019,²⁶ and after the advent of the COVID-19 pandemic, appealed to Congress for a taxpayer-funded bailout.²⁷ In July, USCIS issued furlough notices to 13,400 employees, or nearly 70 percent of its workforce.²⁸ While USCIS delayed furloughs for career staff,²⁹ 800

²⁰ See *Hearing, supra* note 3 (joint written testimony of Don Neufeld, Associate Director, Service Center Operations Directorate, USCIS, and Michael Valverde, Deputy Associate Director, Field Operations Directorate, USCIS).

²¹ AM. IMMIGR. LAW. ASSOC., *USCIS Processing Delays Have Reached Crisis Levels under the Trump Administration* 1 AILA POLICY BRIEF:(2019), www.aila.org/advo-media/aila-policy-briefs/aila-policy-brief-uscis-processing-delays.

²² See Max Greenwood, *Immigration Agency Removing 'Nation of Immigrants' from Mission Statement*, THE HILL, (Feb. 22, 2018), <https://thehill.com/homenews/administration/375112-us-immigration-agency-to-remove-reference-to-us-as-nation-of>; see also U.S. CIT. & IMMIGR. SERV., POLICY ALERT: USCIS PUBLIC SERVICES No. PA-2019-03 (2019).

²³ Asylum Interview Interpreter Requirement Modification due to COVID-19, 85 FED. REG. 59,655, 59,659 (Sept. 23, 2020).

²⁴ See, e.g., *Policy Changes and Processing Delays at U.S. Citizenship and Immigration Services: Hearing before the House Subcomm. on Immigration of the H. Comm. On the Judiciary*, 116th Cong. (2019) [hereinafter *Hearing*] (testimonies of Jill Marie Bussey, Director of Advocacy, CLINIC; Marketa Lindt, President, AILA; Eric Cohen, Executive Director, ILRC, and joint testimony of Don Neufeld, Associate Director, Service Center Operations Directorate, USCIS, and Michael Valverde, Deputy Associate Director, Field Operations Directorate, USCIS).

²⁵ See U.S. Department of Homeland Security, *Citizenship and Immigration Services Ombudsman*, ANNUAL REPORT 2020, at 10-11, www.dhs.gov/sites/default/files/publications/20_0630_cisomb-2020-annual-report-to-congress.pdf (June 30, 2020).

²⁶ U.S. Citizenship and Immigration Services Fee Schedule and Changes to Certain Other Immigration Benefit Request Requirements, 84 FED. REG. 62,280, 62,282 (Nov. 14, 2019).

²⁷ Camilo Montoya-Galvez, *Thousands of U.S. Immigration Agency Employees Could Face Furloughs Without Emergency Funds*, CBS NEWS, (May 26, 2020), www.cbsnews.com/news/u-s-immigration-agency-could-furlough-10000-employees-without-emergency-coronavirus-funds/.

²⁸ U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security, *Deputy Director for Policy Statement on USCIS' Fiscal Outlook* (June 25, 2020), www.uscis.gov/news/news-releases/deputy-director-for-policy-statement-on-uscis-fiscal-outlook.

contracted staff at the agency’s service center in Lee’s Summit, Missouri were furloughed in Sept. 2020 and more are anticipated in the near future.³⁰ To date, USCIS has not received the emergency funding it has sought from Congress to fully address its budget shortfalls and agency leadership maintains that it does not have sufficient funds to maintain its operations beyond the first quarter of FY21. In a recent statement issued by USCIS in response to a preliminary injunction temporarily halting the implementation of its final fee rule, Deputy Director of Policy Joseph Edlow indicated that the injunction “leaves USCIS underfunded by millions of dollars each business day the fee rule is enjoined.”³¹

The NPRM acknowledges that the proposed expansion of surveillance will likely cause costs to rise and budgets to increase as a result yet fails to justify the extra spending or what problems this NPRM aims to solve that requires this level of spending.³² The proposed rule ignores the current USCIS budget crisis and does not detail how USCIS plans to cover the costs associated with this proposal at a time when the agency needs a taxpayer-funded bailout to avoid insolvency – a situation that would lead to further backlogs and a furlough of the majority of its employees. Finally, the NPRM does not adequately describe the alternative and less costly forms of biometrics advancements the agency considered before coming to the conclusions this proposal presents.

Because the NPRM does not sufficiently address this rule’s impact on the ongoing processing delays and budgeting crises at USCIS, we lack the information required to comment meaningfully on the rationale for instituting this regulation and the impacts that it might have on immigrants, refugees, and immigration legal services organizations.

II. DHS’S PROPOSAL TO BROADEN THE DEFINITION OF “BIOMETRICS” AND TO EXPAND ITS BIOMETRIC DATA COLLECTION IS DANGEROUS AND UNJUSTIFIED

CLINIC strongly opposes the proposed increase in the types of biometrics that would be collected about immigrants and others associated with their applications and petitions, as well as to the increased scope thereof. DHS proposes “that any applicant, petitioner, sponsor, beneficiary, or individual filing or associated with a benefit or other request, including U.S. citizens and without regard to age, must appear for biometrics collection, unless DHS or its designee affirmatively decides to not issue a biometrics appointment notice to the individual, or unless DHS waives or exempts the requirement in the form instructions, a Federal Register

²⁹ U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security, *USCIS Averts Furlough of Nearly 70% of Workforce*, (Aug. 25, 2020), www.uscis.gov/news/news-releases/uscis-averts-furlough-of-nearly-70-of-workforce.

³⁰ Daniel C. Vock, *Immigration Agency Cuts of 800 Kansas City Jobs Expected to Trigger Backlogs, Delays Nationwide*, KANSAS REFLECTOR, (Sept. 10, 2020), <https://kansasreflector.com/2020/09/10/immigration-agency-cuts-of-800-kansas-city-jobs-expected-to-trigger-backlogs-delays-nationwide/>.

³¹ U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security, *USCIS Response to Preliminary Injunction of Fee Rule*, (Sept. 30, 2020), www.uscis.gov/news/news-releases/uscis-response-to-preliminary-injunction-of-fee-rule.

³² Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 FED. REG. 56,338, 56,384 (Sept. 11, 2020).

notice, or as otherwise provided by law or regulation.”³³ DHS may waive or exempt the biometrics requirement at its discretion or based on a request for reasonable accommodation.

Immigration policy has seen a steady stream of changes requiring ever more data and information about applicants and those associated with them. On September 11, 2020, the U.S. Court of Appeals for the Second Circuit allowed DHS to resume implementing the Public Charge Ground of Inadmissibility.³⁴ By doing so, DHS can now require more evidence regarding assets, resources, and financial status of the applicant such as their credit report, household assets, and household income.³⁵

Indeed, CLINIC has seen a steady progression of the expansion of data collection during the Trump administration. One example is the indiscriminate collection of social media data—moving away from one-time checks for specific applications and instead seeking broader surveillance. USCIS added a question to ascertain the social media interaction from the last five years to forms DS-260, DS-156, and DS-160.³⁶ It requested that the individual “enter information associated with your online presence, including the types of online providers/platforms, applications, and websites that you use to collaborate, share information, and interact with others. List the username, handle, screenname, or other identifiers associated with your social media profile.” This change produces concerns about freedom of speech since it punishes immigrants for what they share on social media. Although immigrants can limit what they share in their settings on different platforms, they have to be able to read, understand the language, and be familiar enough with the technology to do so, and oftentimes they are asked to share their pages when in the presence of an officer—something that most people would not feel comfortable refusing.

The already-stringent vetting system has been ratcheted up to “extreme vetting,” including use of Automatic License Plate Readers (ALPRs), switching its database to HART, relying on data provided by Palantir, and tracking social media and internet use with an undefined and unlimited scope.³⁷ ALPRs capture license plate numbers that come into view of its camera, and the data are then uploaded to a central server. It is concerning that immigration officers are able to capture such broad information which drivers have no ability to deny given that all vehicles must display a license plate. As the Electronic Frontier Foundation (EFF) has stated “Taken in the aggregate, ALPR data can paint an intimate portrait of a driver’s life and even child First Amendment protected activity. ALPR technology can be used to target drivers who visit sensitive places such

³³ 85 FED. REG. at 56340.

³⁴ 84 FED. REG. 41292 (Proposed Aug. 14, 2019).

³⁵ Ariel Brown, *Guide to Gathering Supporting Evidence for the New USCIS Public Charge Form I-944*, Immigration Legal Resource Center (ILRC) (May 2020), www.ilrc.org/sites/default/files/resources/guide_to_collecting_evidence_for_uscis_public_charge_form_i-944.pdf.

³⁶ 83 FED. REG. 43952 (Proposed Aug. 28, 2018).

³⁷ Joan Friedland, *Information Vacuuming, The Trump Administration is Collecting Massive Amounts of Data for its Immigrant Surveillance and Deportation Machine*, National Immigration Law Center (NILC) (Aug. 22, 2018) www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/.

as health centers, immigration clinics, gun shops, union halls, protests, or centers of religious worship.”³⁸

The infringement on civil liberties due to increased monitoring is not justified by DHS’s claim that they are transitioning to a “person-centric” model. DHS fails to justify why this model is needed and does not provide data on any deficiencies with the current standard of practice. The claim that “biometrics are unique to each individual and provide USCIS with tools for identity management” does not address challenges with the systems and their algorithms producing false identifications, nor does it discuss privacy or other constitutional concerns, or accurately estimate the costs of these changes. DHS’s desire to expand immigrant surveillance after already instituting “extreme vetting” poses questions as to how much vetting will finally be enough, and where the infringement of civil liberties will end.

a. DHS Has Not Justified Expanding its Biometric Data Collection.

The NPRM does not explain why DNA collection is necessary and why current measures are inadequate. In the introduction to the proposed rule, DHS outlines why it currently collects biometric information.³⁹ Yet its next step is to revert to a backward argument in an attempt to justify its need to expand the range of sources of biometric information. DHS emphasizes that it “is precluded in many cases from approving, granting, or providing immigration benefits to individuals with a record of certain criminal offenses or administrative violations.”⁴⁰ That DHS is legally precluded from approving benefits without particular information does not mean that the agency is unable at present to function adequately. The argument, more implication than explication, restates DHS’s data collecting role, but now with a more ominous shading. DHS insinuates that it operates on a thin edge: if it does not get all the information that the rule demands, then the agency will fall short of its lawful duties. The wording is designed to be alarming, and it is, but not for the intended reasons. DHS appears to suggest that it must have its new rule because it is failing in its statutory obligation to screen immigrant applicants for benefits. This type of contorted argumentation, reproduced throughout the rule, evinces the proposal’s weakness.

Furthermore, DHS’s precautions against crime are supposed to target possible perpetrators, not impinge on the innocent. The proposed rule does not demonstrate that DHS’s current set of biometrics is inadequate for its purposes, nor does it give evidence that the proposed sweeping biometric methods will measurably reduce crime against immigrants. The present criminal

³⁸ Electronic Frontier Foundation, *Automated License Plate Readers (ALPRs)*, (Most recently updated Aug. 28, 2017), www.eff.org/pages/automated-license-plate-readers-alpr.

³⁹ “DHS currently collects, stores, and uses biometrics for the following purposes: Conducting background checks to determine eligibility for a benefit or other request; document production associated with an application, petition, or other request for certain immigration and naturalization benefits or actions; and performing other functions related to administering and enforcing the immigration and naturalization laws such as identity verification upon issuances of a Notice to Appear (NTA) under section 240 of the INA.” 85 FED. REG. 56338, 56339. The proposed rule does not point to any legislative changes to the INA that compel the agency to modify its present data collection.

⁴⁰ 85 Fed. Reg. at 56339, 56347, 56349, 56352, 56354.

identification and arrest practices have apparently been fruitful for years—indeed, so much that they have ignited international consternation and calls for reform.⁴¹

The proposed rule summarizes its goal in a few chilling sentences that reveal DHS’s overreach and its lack of concern for basic rights:

For biometrics use to expand *identity management and verification in the immigration lifecycle*, this rule would allow for biometrics collection from *any individual, without age limitations*; thus, DHS proposes to *remove all age limitations or restrictions on biometrics collection from the regulations* in the context of both immigration benefits requests, entering or *exiting* the United States, NTA issuance, and *to perform other functions related to administering and enforcing the immigration and naturalization laws*.⁴²

Each of these purposely vague but portentous phrases is dismaying. All together, they portray an agency that has lost track of its role.

The rule’s frequent circumlocutions and weighted prose betrays DHS’s confusion about its identity. DHS misunderstands its role and its legal boundaries when it proposes to become the national repository of genetic information on all immigrants and many current U.S. citizens. DHS insists on erecting its own elaborate database, although it never explains why it cannot resort to data kept by the FBI.⁴³ It insists that it needs to keep a pace with the FBI—with whom it will readily share whatever data it assembles.⁴⁴ The rule simply asserts that DHS must have an abundance of data on all immigrants, regardless of any documented criminal history (and regardless of age). Its closest attempt at an explanation is a complaint about the processing times that the legacy Immigration and Naturalization Service (INS) had to endure in the 1990s when working with the FBI.⁴⁵ Traction in government data sharing is thus a central reason behind DHS’s desire to do its own expansive biometric harvesting. But inefficiencies in government operations do not justify intrusions on personal rights.

b. The Proposed Redefinition of “Biometrics” Gives the Federal Government Perilous Access to Individuals’ Genetic Information.

DNA is not merely a personal marker of one person’s genetic makeup. DNA is passed on to progeny. As such, it is also traceable in reverse; one’s genes can reveal much about one’s

⁴¹ Inter-American Commission on Human Rights, Organization of American States, REPORT ON IMMIGRATION IN THE UNITED STATES: DETENTION AND DUE PROCESS, (2010).

⁴² 85 FED. REG. at 56342 (emphases added).

⁴³ 85 FED. REG. at 56342, 56355.

⁴⁴ “Generally, DHS plans to use the biometric information collected from children for identity management in the immigration lifecycle only, but will retain the authority for other uses in its discretion, such as background checks and for law enforcement purposes. DHS does not intend to routinely submit all UAC or AAC biometrics to the FBI for criminal history background checks; rather, the biometrics collected from the majority of these children would be stored in IDENT to help DHS with future encounters. USCIS is authorized to share relevant information with law enforcement or other DHS components, including “biometrics” for identity verification and, consequently, it may share DNA test results, which include a partial DNA profile, with other agencies as it does other record information pursuant to existing law.” 85 FED. REG. at 56352.

⁴⁵ 85 FED. REG. at 56349.

forebears. Many of the immigrants who arrive in the United States today will become U.S. citizens, and the progenitors of citizens.

The science of genetic decryption is getting ever better. Genetic data can already be studied to detect characteristics that are often categorized as “ethnic” or “racial” markers. DHS recognizes this.⁴⁶ With enactment of the proposed rule, DHS would start building a library of genetic data that will grow indefinitely, and that DHS intends to retain into perpetuity.⁴⁷ Through the proposed rule, DHS would become host to ever more genetic data of ever more U.S. citizens. However, serving as the federal repository of genetic information of a huge portion of the population, including U.S. citizens, is not DHS’s prescribed function.

What distinguishes the federal government from Ancestry.com or 23andme⁴⁸ is not so much the companies’ pursuit of profit. Rather, it is that the government enacts laws. Thanks to the proposed rule, the federal government, engorged with DNA collected from millions of individuals, could one day pass laws targeting genetic characteristics. It is hardly unknown for the United States or other modern states to propound legal differentiations within their citizenry. In fact, abuses of genetic notions have fed all too many campaigns of decimation. While the science may have been less sophisticated in the past, that is beside the point. What matters is what information is available, and thus susceptible, to political exploitation. Oppressive governmental policies, no less than popular racism, can feed on scientific information. Such information can provide governments a potent and convincing tool for iniquitous efforts.⁴⁹ Nor

⁴⁶ 85 FED. REG. at 56355.

⁴⁷ DHS expresses its intent to keep such records in the proposed rule. For example, it wants to acquire biometrics, now writ-large to include DNS, “to ensure that necessary adjustments can be made to meet emerging needs.” 85 FED. REG. at 56339. Throughout the proposed rule, DHS notes that it “collects and stores” biometric information. When it speaks of “immigration lifecycle,” it does not suggest that data will be discarded at the end of each “lifecycle,” however the agency understands it.

⁴⁸ These private, legal businesses have already proven to be problematic. Charles Seife, *23andMe Is Terrifying, but Not for the Reasons the FDA Thinks*, SCIENTIFIC AMERICAN, Nov. 27, 2013), www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-the-reasons-the-fda-thinks/.

⁴⁹ “Certification whether a person is of Aryan background lies solely within the authority of experts in race research employed in the Interior Ministry.” (“Für Gutachten darüber, ob eine Person arischer Abstammung ist, kommt nur der Sachverständige für Rassenforschung beim Reichsministerium des Innern in Frage.”). (Author’s translation) MINISTERIALBLATT FÜR DIE PREUSSISCHE INNER VERWALTUNG, Column 416, Oct. 29, 1934, in DAS SONDERRECHT FÜR DIE JUDEN IM NS-STAAAT, 2nd Edition, Joseph Walk (ed.) UTB für Wissenschaft/C.F. Mueller Verlag, 1996, Heidelberg at 95, #468. This order was promulgated by the *Landesregierung* of the Free State of Prussia, created in 1918. The edict preceded the issuance of the *Reichsgesetz*, passed by the Nazi national government on September 15, 1935. The Nazis began officially dissolving the various German Free States in 1934.

The *Reichsbürgergesetz* of 1935 distinguished between German citizens (*Reichsbürger*) and everyone else living in Germany. The differentiation was rooted variously in “blood” and “Aryan descent.” The consequences of the distinction were profound from the beginning, and became only more invidious as the law developed over the following years:

1. A Reich citizen is a subject of the state who is of German or related blood, and proves by his conduct that he is willing and fit to faithfully serve the German people and Reich.
2. Reich citizenship is acquired through the granting of a Reich citizenship certificate.
3. The Reich citizen is the sole bearer of full political rights in accordance with the law.

can we be sanguine about some purported higher level of American moral wisdom over that of other countries.⁵⁰ DHS is seeking the capability to gather more sensitive personal biological information at the very time when the specter of White Supremacy has become brazenly public and the President praises constituents for the quality of their genes.⁵¹ That the government would have these data, not only for those who were sampled, but for their descendants, too. History does not reassure that governments are always disinterested in the supposed genetic well-being of their U.S. citizens and other residents.⁵² Genetic, or proto-genetic, distinctions have had a

RGB I (REICHSGESETZBLATT) S. 1146, (Sept. 15, 1935.) (Translation from the ENCYCLOPEDIA OF THE HOLOCAUST), <https://encyclopedia.ushmm.org/content/en/article/nuremberg-laws>.

The *Reichbürgergesetz* was amended two months later to delineate with more precision the substrate for the legal differentiation between Reich citizens and others, in particular, Jews. The legal basis for the distinction was a mixture of racial background and social identity:

Sec. I

(1) Pending passage of additional regulations concerning the Reichsbürgerbrief, citizens of the Reich are provisionally determined to be citizens of German or related (*artverwandten*) blood, who, with the legal passage of the Reichsbürgergesetz, possesses the right to vote, or to whom the Interior Minister of the Reich, with the agreement of the Deputy of the Führer, grants provisional Reich's citizenship right.

(2) The Interior Minister of the Reich can, in agreement with the Deputy of the Führer, remove the provisional Reich's citizenship right.

Sec. II

(1) The regulations of Section (1) also apply to citizens of mixed Jewish and non-Jewish background.

(2) A Jewish *Mischling* is anyone who has one or two grandparents of full Jewish racial background, insofar as he does not qualify as a Jew under Sec. 5, paragraphs 2. A grandparent also qualifies as full-Jewish if he had been a member of the Jewish religious community.

RGB I S. 1333, (Nov. 14, 1935) (Author's translation), <http://alex.onb.ac.at/cgi-content/alex?apm=0&aid=dra&datum=19350004&seite=00001333&zoom=2>. Sec. V breaks down the subcategories of *Mischlinge* in more detail.

⁵⁰ Indeed, U.S. discriminatory practices, both toward its own citizens and immigrants, provided cross-pollination for other countries' practices. One historical example is extensively traced in James Q. Whitman, *HITLER'S AMERICAN MODEL: THE UNITED STATES AND THE MAKING OF NAZI RACE LAWS* (Princeton University Press, 2017).

⁵¹ Ashley Parker, *Trump brings divisiveness and invective back to the rally stage*, WASHINGTON POST, (Sept. 28, 2020), www.washingtonpost.com/politics/trump-rallies-divisive/2020/09/28/a5114d68-fea8-11ea-830c-a160b331ca62_story.html. At a rally in Minnesota on September 18, Trump said, "You have good genes, you know that, right? You have good genes. A lot of it's about the genes, isn't it? Don't you believe that? The racehorse theory — do you think we're so different? You have good genes in Minnesota;" Maya Rao, *Trump's 'good genes' comment at Bemidji rally draws condemnation*, STAR TRIBUNE, (Sept. 21, 2020), www.startribune.com/trump-s-good-genes-comment-at-bemidji-rally-draws-condemnation/572486371/.

⁵² See Gesetz zur Verhütung erbkranken Nachwuchses, (Jul. 14, 1933), REICHSGESETZBLATT I S. 529 (in der Fassung vom Apr. 2, 1936), REICHSGESETZBLATT I S.119, reproduced in Ingo von Münch, ed., *GESETZE DES NS-STAATES*, (3rd ed., UTB für Wissenschaft/Ferdinand Schöningh, 1994) at 113. The national law ordained that, "Whoever suffers from a genetic disease can be made infertile (sterilized) if, in accordance with the determinations of medical science, it can be anticipated, with a high probability, that his children will suffer severe physical or mental hereditary disabilities." RGB I S. 529, Sec. 1(1) (Author's translation). Section 1(2) of the statute listed the hereditary diseases covered by the statute, including intellectual disabilities, schizophrenia, manic-depression ("circular insanity"), epilepsy, Huntington's chorea, inherited blindness or deafness, and physical malformation. Section 1(30) separately designated "severe alcoholism" as another proscribed genetic vulnerability.

notorious role in this country's legal history, for U.S. citizens and for immigrants alike.⁵³ The federal government targeted immigrants—to their detriment—according to ethnicity and national origin, with the rationale that it is protecting the country's safety.⁵⁴

Still another evident, but unacknowledged, hazard harbored in the proposed rule is that it would make DHS privy to information about individual's genetic health conditions. The agency could conceivably resort to its expanded biometric database as a tool for determinations of admissibility under INA Section 212(a)(2)(A)(iii). Although the INA Section 212(a)(1)(2)(i) speaks of "communicable diseases of public health significance," the revision or reinterpretation of that language to include hereditary conditions is not unimaginable. And, DHS intends to share the data in its DNA treasure trove with other agencies. The potential for future harm is evident and worrying.

Through the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Nondiscrimination Act (GINA), federal law mandates strict privacy and security ligatures around the collection and handling of genetic information by private concerns. However, the degree of precaution embodied in those statutes is not matched by legal strictures on the government's own treatment of genetic data. There are restrictions on inter-agency information sharing of personal identification information (PII) and other private information.⁵⁵ Nevertheless, the law still lags when it comes to intra-governmental safeguards for the use of genetic data in relation to health conditions.

The federal government has repeatedly experienced severe breaches in its storage of PII. The Government Accountability Office (GAO) reviewed DHS's data security practices a few years ago and found them to be in perpetual jeopardy:

Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by the National Institute of Standards and Technology (NIST) has identified 82,384 publicly known cybersecurity vulnerabilities and exposures as of February 9, 2017, with more being added each day. Federal systems and networks are also often interconnected with other internal and external systems and networks including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.⁵⁶

⁵³ Kevin R. Johnson, *The New Nativism*, in Juan F. Perea, ed., *IMMIGRANTS OUT!: THE NEW NATIVISM AND THE ANTI-IMMIGRANT IMPULSE IN THE UNITED STATES*, (New York University Press, 1997) at 165ff.

⁵⁴ Jennifer M. Caçon, *The Security Myth: Punishing Immigrants in the Name of National Security*, in Julie A. Dowling and Jonathan Xavier Inda, *GOVERNING IMMIGRATION THROUGH CRIME: A READER*, (Stanford University Press, 2013) at 77ff.

⁵⁵ For example, the Internal Revenue Code inter-agency use of tax filing information is regulated strenuously, per 26 USC Section 6103.

⁵⁶ The GAO testimony continued:

But, despite GAO’s calls for DHS to improve its data security, and DHS’s own apparent commitment to shoring up its protections, the agency’s failures in this area continue.⁵⁷ In a very recent incident, one of the DHS’s private subcontractors “directly violated DHS security and privacy protocols” involving a new facial recognition technology pilot project. What matters here is not that DHS had such policies, but that it had the facial recognition data—and its policies did not prevent the breach.

c. DHS Has Not Sufficiently Addressed Data Security or the Agency’s History of Data Breaches.

The proposed rule goes into great detail regarding the types of personal data that may be collected and from whom, but it only briefly mentions the data security concerns that are inherent in this unprecedented level of surveillance.

The proposed rule does not explicitly state where DHS plans to store the vast amounts of biometric data it will collect. Currently, DHS biometric data are stored in IDENT under the auspices of the Office of Biometric Identity Management (OBIM). Going forward, these data will be stored in DHS’s new HART database, which raises serious concerns regarding its information-sharing and use.⁵⁸

In addition, cyber threats to systems supporting the federal government and critical infrastructure are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Risks to cyber assets can originate from unintentional and intentional threats. These include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Ineffectively protecting cyber assets can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety.

Cybersecurity: Actions Needed to Strengthen U.S. Capabilities, Statement of Gregory C. Wilshusen to the House Subcommittee on Research and Technology, Committee on Science, Space, and Technology, (Feb. 14, 2017), www.gao.gov/assets/690/682756.pdf. Dell Cameron, *Homeland Security Data Breach Affects 240,000 Federal Employees, Plus Witnesses and Interviewees*, GIZMODO, (Jan. 3, 2018), <https://gizmodo.com/homeland-security-data-breach-affects-240-000-federal-e-1821755817> and Tom Brant, *Breach Exposes Data from Thousands of DHS Employees*, PC MAGAZINE DIGITAL EDITION, (Feb. 8, 2016), www.pcmag.com/article2/0,2817,2499013,00.asp; <https://gizmodo.com/homeland-security-data-breach-affects-240-000-federal-e-1821755817>.

⁵⁷ Office of the Inspector General, U.S. Department of Homeland Security, *Review of CBP’s Major Cyberspace Incident During a 2019 Biometric Pilot*, (Sept. 21, 2020), www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

⁵⁸ U.S. Department of Homeland Security (DHS), *Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA)*, 2, DHS/OBIM/PIA-004 (February 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf. [hereinafter *HART PIA*].

HART, the world's second largest biometric system,⁵⁹ will be hosted by Amazon Web Services' GovCloud (AWS), and it "stores and processes biometric data."⁶⁰ The database will contain "centralized DHS-wide biometric" data, as well as more limited contextualizing biographic and encounter history data. According to the HART Increment 1 Privacy Impact Assessment, a HART record may include biometric data, biometric-associated biographic data, derogatory information (DI), officer comments, encounter data, and machine-generated identifiers. These broad categories include the following information:

- Biometric data
- Biographic data: full name, aliases, date of birth, gender, physical identifying details, signature, assigned number identifiers;⁶¹
- DI: warrants, known or suspected terrorist (KST) designations, sex offender registrations, foreign criminal convictions, immigration violations;⁶²
- Officer comment information: only when available;
- Encounter data: the location and circumstance of each instance of biometric data collection; and
- Unique machine-generated identifiers: identifiers generated by HART such as Fingerprint Identification Number (FIN) and Encounter Identification Number (EID) that link these various records.⁶³

This proposed rule allows biometrics to be fed into HART on a large scale without the necessary privacy impact assessments having been conducted—making the lack of any reference to HART in the text of the proposed rule particularly concerning. DHS has only conducted a privacy impact assessment (PIA) for the first increment of HART (which is rolling out in four increments).⁶⁴ The Increment 1 PIA indicates that "Increment 2 will provide additional biometric capabilities to HART to meet customer needs;" a PIA has therefore not yet been conducted for functionalities within the overall design of HART that implicate the data that are the subject of this rule. Through this rule, then, DHS would slip a vast array of data into a system without a prior privacy impact assessment concerning its processing and use.

HART will also make it possible to share this information at a large scale, circumventing traditional points of oversight or limitation. For example, Customs and Border Protection's (CBP) Analytic Framework for Intelligence (AFI) collects information from internet and social media sources, and HART shares personally identifying information with a feeder database for

⁵⁹ C Burt, *Inside the HART of the DHS Office of Biometric Identity Management*, BIOMETRIC UPDATE (Sep 2018), www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management.

⁶⁰ U.S. Department of Homeland Security, *Privacy Threshold Analysis (PTA) for Homeland Advanced Recognition Technology (HART) Development Testing Environment (DTE)* (Apr 2015), produced as part of EPIC-18-06-18-DHS-FOIA-20190422-Production, available at <https://epic.org/foia/dhs/hart/EPIC-2018-06-18-DHS-FOIA-20190422-Production.pdf> [hereinafter *DHS HART DTE PTA*] at 6.

⁶¹ The HART Increment 1 PIA lists these as including: A-Numbers, SSN, state ID number, civil record number, agency-specific fingerprint record locator information, FBI Number, EID, DoD Biometric Identifier (DOD BID), National Unique Identification Number (NUIN), passport or visa data, and citizenship and nationality documents. *HART PIA*, *supra* note 58.

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*

AFI.⁶⁵ CBP also operates as a data provider to HART. It has stated that it plans to expand database capabilities to include access to commercially ALPR information.⁶⁶ Commercial aggregators collect license plate information from private businesses, local governments, law enforcement agencies, and financial institutions (typically via repossession companies) and then these aggregators “store, index, and sell access to the images and time and location of collection.”⁶⁷ CBP has itself noted the potentially negative effects of the use of ALPR data, which can potentially provide information about constitutionally protected activities such as “travel over time ... [or] an individual’s private life, such as frequenting a place of worship or participating in protests and meetings.”⁶⁸ CBP claims its structure mitigates civil liberties and privacy concerns, but still, for example, allows users to query historical ALPR data up to five years old.⁶⁹

HART also allows for more interoperability between U.S. databases and even foreign databases. FBI, DHS, and DOD announced that they are introducing new standards that allow their major biometric databases to “communicate natively, ‘in their own language.’”⁷⁰ The Electronic Biometric Transmission Specification (EBTS) version 4.1 will, or does, allow the Automated Biometric Information System (DOD), Next Generation Identification (FBI), and IDENT/HART (DHS) greater transactional interoperability. EBTS is “also compatible with NATO’s STANAG 4715 ... enabling information sharing with foreign partners.”⁷¹ The disastrous effects of information sharing between inaccurate, biased, and unreliable law enforcement databases and immigration databases has been extensively documented.⁷² Information stored in unreliable and secretive gang databases has been used to deny asylum claims and separate families.⁷³ For example, CBP has relied on data via a transnational intelligence-sharing program, involving Mexico, El Salvador, Guatemala, and Honduras to make determinations to tear families apart.⁷⁴

⁶⁵ *DHS HART DTE PTA Replacement Biometric System Increment 1*, *supra* note 60, at 6-8,

⁶⁶ Customs and Border Protection, U.S. Department of Homeland Security, *Privacy Impact Assessment Update for the Automated Targeting System*, DHS/CBP/PIA-006(e), 77, (Jan. 13, 2017), www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-may2020.pdf [hereinafter *CBP ATS PIA Update*].

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ Chris Burt, *U.S. agencies working on standard for seamless communication between biometric databases*, BIOMETRIC UPDATE (Sept. 26, 2018), www.biometricupdate.com/201809/u-s-agencies-working-on-standard-for-seamless-communication-between-biometric-databases.

⁷¹ *Id.*

⁷² In *Gonzalez v. ICE*, for example, the Ninth Circuit has held that, in their enforcement actions, ICE has relied on databases with large gaps in necessary data that have significant error rates in the data they contain. See *Explaining the Gonzalez v. ICE Injunctions*, Immigrant Legal Resource Center, (Oct. 2019), www.ilrc.org/sites/default/files/resources/2019.11_ilrc_gonzalez_v_ice-11.07.pdf. See also Joan Friedland et al., *Untangling The Immigration Enforcement Web*, National Immigration Law Center, (Sept. 2017), www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

⁷³ Melissa del Bosque, *Immigration Officials Use Secretive Gang Databases to Deny Migrant Asylum Claims*, PROPUBLICA, (July 8, 2019), www.propublica.org/article/immigration-officials-use-secretive-gang-databases-to-deny-migrant-asylum-claims.

⁷⁴ See Jesse Franzblau, *Family Separation Policy Continues, New Documents Show*, National Immigrant Justice Center, (June 22, 2019), <https://immigrantjustice.org/staff/blog/family-separation-policy-continues-new-documents-show>. DHS officials have separated families on the basis of unsubstantiated information shared from foreign governments. See U.S. House Judiciary Committee Hearing Oversight of Family Separation and U.S. Customs and Border Protection Short-Term Custody under the Trump Administration, Statement of the National Immigrant

With the vast expansion of information collection contemplated by this rule, these problems could increase.

Not only is there no way to ensure that information fed into the databases “communicating” with HART is accurate, the implications of biometrics being stored in HART, and that data shared with foreign governments, is particularly alarming for immigrants who have a fear of persecution in their home countries or who were subject to trafficking. The rule contains no information on how information sharing will be limited to protect against data falling into the wrong hands.

But the concerns regarding the retention, management, and use of data stored in the HART system do not stop there. Data retention and review in HART is managed by data owners and providers, not DHS’s OBIM. OBIM freely admits that the risk of providers not properly managing their data is unmitigated.⁷⁵ Because this data are owned by the providers rather than OBIM, OBIM only recommends that providers follow certain standards rather than being able to verify the accuracy, completeness, and quality of the data composing HART.⁷⁶ There is also concern that data, once provided, will not be accurately maintained, since data providers must manually update DI and information related to case disposition.⁷⁷

OBIM also concedes that facial image matching results may be disproportionately inaccurate, particularly in certain racial groups.⁷⁸ Notably, the External Biometric Records (EBR) database that populates HART has been exempted from Privacy Act requirements on accuracy, which, as the World Privacy Forum has stated, “is remarkable for a system that will have a high impact on individuals’ civil liberties.”⁷⁹ The rule makes reference to the accuracy of biometrics and the speeding up of processes in an automated biometric system, but the risk of reliance on inaccurate biometric results, including facial recognition results, in a system that provides no fast and easy redress for misinformation is particularly high under this new rule.

The proposed expanded definition of biometrics and HART’s inclusion of “encounter data” could have a chilling effect on the exercise of constitutionally guaranteed rights, as this data includes information on the “location and circumstance of each instance resulting in biometric collection.”⁸⁰ Although not a stated purpose in any of the HART or associated systems documents, the collection, storage, and potential future dissemination of location and

Justice Center (NIJC), (July. 25, 2019), www.congress.gov/116/meeting/house/109852/documents/HHRG-116-JU00-20190725-SD014.pdf.

⁷⁵ National Immigration Law Center and Just Futures Law, *Comments on Privacy Act of 1974; New System of Records Titled “Department of Homeland Security/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records (SOR)” and Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records*, 29 (May 2020), www.regulations.gov/document?D=DHS-2019-0047-0004.

⁷⁶ *HART PIA*, *supra* note 58.

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ World Privacy Forum, *Comments of World Privacy Forum to Department of Homeland Security regarding Proposal to Establish a New DHS System of Records*, U.S. Department of Homeland Security/ALL-041 External Biometric (EBR) System of Records and Proposal to Exempt New DHS External Biometric (EBR) from Key Provisions of the Privacy Act of 1974, 3 (May 25, 2018), www.regulations.gov/document?D=DHS-2017-0040-0005.

⁸⁰ *HART PIA*, *supra* note 58, at 16.

circumstance data allows DHS and other partners to potentially track individuals' movements and the exercise of their rights. As the National Immigration Law Center and the National Immigration Project of the National Lawyers Guild have noted, the use of these encounter data along with other included biographic and biometric data allows HART to “manufactur[e] profiles of individuals, with little accountability or attention to privacy and accuracy.”⁸¹

The proposed rule states that USCIS “has internal procedural safeguards to ensure technology used to collect, assess, and store the different modalities is accurate, reliable and valid.”⁸² Yet these are not expanded on and problems in existing DHS databases⁸³ indicate that they are not sufficient to protect against misidentification or data protection violations. Challenging flawed information in HART is procedurally cumbersome and only possible for U.S. citizens, lawful permanent residents, and other individuals covered under the Judicial Redress Act.⁸⁴

Further, the proposed rule impacts information collected in other databases, because, through IDENT and ultimately through HART, data collected under this rule is fed into a web with other databases, including the FBI's Next Generation Identification system. As noted above, the rule also contemplates the use of facial recognition technology on facial images.⁸⁵ By applying new technologies and analytical methodologies to data that were previously collected, the proposed rule violates the prohibition on retroactivity in rulemaking.⁸⁶ Individuals who gave their consent for data collection in other contexts, and rules that allowed for data collection without consent, did not anticipate this very broad use of their data under new technological systems.

The NPRM acknowledges that individuals who submit biometrics could have concerns about data security and breaches.⁸⁷ However, it does not mention or consider that such concerns rise above and beyond standard security concerns due to the addition of DNA requests, which traditionally are not considered part of biometrics, and DHS' history of data insecurity and breaches. As discussed below, the expansion of the modalities of biometrics to include DNA is cause for significant privacy concern, not only for data and identity security, but for health and medical privacy as well, with an agency not intended for medical data management. Further, privacy concerns about DNA and all other biometric data covered by this proposed rule are amplified due to DHS' history of poor data management and data security breaches. For example, in May 2019, a CBP biometrics database was breached, and traveler data including

⁸¹ National Immigration Law Center and National Immigration Project of the National Lawyers Guild, *Comments on Notice of a New System of Records: Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records*, 3 (May 23, 2018), www.regulations.gov/document?D=DHS-2017-0040-000.

⁸² 85 FED. REG. at 56355.

⁸³ In *Gonzales v. Immigration and Customs Enforcement (ICE)*, the Court found current government immigration databases to be “largely erroneous” and of “dubious reliability,” and held that “the collection of datapoints ICE gathers from the various databases does not provide affirmative indicia of removability to satisfy probable cause determination because the aggregation of information ICE receives from the databases is largely erroneous and fails to capture certain complexities and nuances of immigration law.” See *Gonzales v. Immigration and Customs Enforcement*, 126, (C.D. Cal 2019), www.immigrantjustice.org/sites/default/files/content-type/press-release/documents/2019-09/gonzalez-v-ice_20190927_decision.pdf.

⁸⁴ *HART PIA*, *supra* note 58, at 34-35.

⁸⁵ 85 FED. REG. at 56356.

⁸⁶ See *Bowen v. Georgetown University Hospital*, 488 U.S. 204 (1988).

⁸⁷ 85 FED. REG. at 56388.

images from a facial recognition program were compromised.⁸⁸ There is no indication that security at DHS is improving after breaches such as this. In fact, the DHS Office of Inspector General’s report on the information security program for FY 2019 found that DHS’s information security had regressed compared to previous years.⁸⁹

d. DHS’s Proposed Redefinition of “Biometrics” Exceeds the Agency’s Legal Jurisdiction.

DHS maintains early on that it has legal authority under the INA to gather biometric information from immigrants applying for specified benefits.⁹⁰ That claim by itself is misleading. Further on, DHS’s wish list of modifications to the biometrics definition prove that DHS has overstated its authority. Neither the statute nor the pertinent controlling regulation gives the agency the authority for such overreach.⁹¹ The rule both implies that DHS already has the authority to strengthen its biometric requirements, and yet appeals for the expansion.

The proposed rule’s extension of DNA collection to U.S. citizens who are petitioning for qualifying family members living abroad would have predictable deleterious consequences that the rule overlooks.⁹² The rule would make such a decision fraught and would compel families—inside and outside the country—to second-guess the prudence of family reunification if it requires disclosure of unreasonable amounts of private data to government databases. U.S. citizens would face the dilemma of supporting their relatives’ immigration and their concern about keeping their DNA out of government hands. Unless the federal government demands DNA from every citizen, a rebarbative prospect, the proposed rule would engender a division among U.S. citizens: those whose DNA is held in federal records and those whose DNA remains private.

e. The Proposed Rule Violates the Fourth Amendment Prohibition Against Unreasonable Searches.

By collecting people’s most personal, immutable biological information, DHS would be accruing records that could have the deepest consequences if abused. No information is more specific to a person than their own DNA. Furthermore, the genetic information of one person can be researched to reveal information about that person’s relatives. The web of people who could suffer from mishandling of genetic data is broad and multigenerational. Including DNA as a biometric produces legally drastic repercussions. While faces may be unique (although we all note inherited features), DNA endures. It is not confined just to the individuals who provide the evidence but to their descendants and relatives. By gathering DNA information, DHS would be accruing records for the government that could be consequential for generations to come.

⁸⁸ See Office of Inspector General, U.S. Department of Homeland Security, *Review of CBP’s Major Cybersecurity Incident during a 2019 Biometric Pilot*, (Sept. 21, 2020), www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

⁸⁹ See Office of Inspector General, U.S. Department of Homeland Security, *Evaluation of DHS’ Information Security Program for Fiscal Year 2019 (REDACTED)*, (Sept. 30, 2020), www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-20-77-Sep20.pdf.

⁹⁰ 85 FED. REG. at 56339.

⁹¹ 8 CFR Sec. 103.16

⁹² 85 Fed. Reg. at 56348.

DNA collection raises significant privacy and Fourth Amendment concerns. Since 2013, the U.S. Supreme Court’s decision in *Maryland v. King* has permitted law enforcement to collect DNA samples based on their arrests or convictions for certain criminal offenses. Efforts of some states to expand the collection of DNA to persons arrested for lower level offenses have been met with great concern.⁹³ No subsequent law, however, permits authorities to collect DNA samples from U.S. citizens and non-citizens who have not been arrested by law enforcement authorities or detained by ICE.

The agency does not address these serious matters in its proposed rule. The agency believes that the rule does not create new privacy concerns but merely expands the population affected by privacy concerns.⁹⁴ Even if that were so, the agency makes no effort to allay concerns related to privacy and overreach. It does not propose any measures that would lessen the impact of the rule where less invasive measures of identity verification are available and sufficient, such as supervisory review of DNA requests, any threshold of evidence short of DNA collection that would satisfy requirements, a provision requiring informed consent, or any protocol for the evaluation of test results reported by the government. By extending to DHS broad, unreviewable discretion to determine when DNA collection should be required and analyzed, the proposed rule fails utterly to respond to these important and relevant policy concerns.

Similar expansions of DNA collection in other countries have been recognized as disproportionate and a violation of rights, and courts across Europe, the Middle East,⁹⁵ and Africa,⁹⁶ have struck down such systems, leading to a waste of public resources in the creation of these systems. In 2018, for example, the European Court of Human Rights reached a unanimous judgment in a case against the UK on DNA collection, holding that “the retention [of DNA, biological samples and fingerprints] constitutes a disproportionate interference with the applicants’ right to respect for private life and cannot be regarded as necessary in a democratic society.”⁹⁷ In response to the judgment and debate around the issue of DNA collection, the Protection of Freedoms Act 2012 came into force in England and Wales, which saw the removal

⁹³ See, e.g., Bill Farrar, *Proposal to Expand Mandatory DNA Collection in Virginia Raises Serious Privacy and Due Process Concerns*, ACLU FREE FUTURE BLOG (Jan. 8, 2018), www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/proposal-expand-mandatory-dna-collection (noting that a proposal in Virginia would have added “obstruction of justice” and “shoplifting” to the list of misdemeanor offenses that authorized DNA collection).

⁹⁴ 85 FED. REG. at 56343. (“There could be some unquantified impacts related to privacy concerns for risks associated with the collection and retention of biometric information, as discussed in DHS’s Privacy Act compliance documentation. However, this rule would not create new impacts in this regard but would expand the population that could have privacy concerns.”).

⁹⁵ In 2017, a court in Kuwait found that the collection of DNA samples of citizens and visitors of Kuwait by the government violated constitutional provisions on personal liberty and privacy, see Human Rights Watch, *Kuwait court strikes down draconian DNA law*, (Oct. 2017), www.hrw.org/news/2017/10/17/kuwait-court-strikes-down-draconian-dna-law.

⁹⁶ A High Court in Kenya struck down the collection of DNA in the context of a biometric digital ID system earlier this year, High Court of Kenya at Nairobi, *Nubian Rights Forum & 2 others v Attorney General & 6 others; child Welfare Society & 9 others (interested parties)* [2020] eKLR, (Jan 2020), <http://kenyalaw.org/caselaw/cases/view/189189/>.

⁹⁷ *Marper v. The United Kingdom*, Eur Ct H. R., (2008), <https://rm.coe.int/168067d216>.

of over 1.7 million DNA profiles of innocent people and children and the destruction of close to 8 million DNA samples.⁹⁸

Agencies are not supposed to write whatever they desire and then await possible litigation for the courts to correct their excrescences. These interpretative standards are not solely the tools of the courts. Rather, agencies should prepare their regulations in keeping with the law, just as Congress is to compose legislation that does not trespass on constitutional rights. DHS gave insufficient thought to the reasonable bounds of its proposed data collection.

f. DHS Should Discontinue the Use of Facial Recognition Technology, as It is Unreliable, Particularly as Applied to Diverse Faces.

The government itself has flagged deeply troubling issues as recently as December 2019, when a study from the National Institute of Standards and Technology showed that facial-recognition systems falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces.⁹⁹ There were also difficulties identifying women, children, and older adults.¹⁰⁰ That means that communities which are already disenfranchised are more likely to be misidentified. The FBI and ICE have already been using state driver's license databases to search through millions of photos.¹⁰¹ DHS seeks to weaponize this substandard technology for overreaching surveillance.

An expanded facial recognition system would also pave the way for mass, pervasive, continuous surveillance without cause, particularly if information-sharing across multiple databases is enabled. A database with facial recognition capabilities of primarily brown and Black immigrants and their family members—who are already likely to be over-policed compared to the rest of the population—could easily lead to their false identification through information-sharing with criminal databases, which are accessed by state, local, and federal law enforcement agencies. There is simply no justification provided for this far-reaching use of facial recognition technology when less-invasive methods including identification via photograph or fingerprint are available.

g. DHS Should Withdraw Its Proposal to Collect Photographs of Anatomical Features.

DHS proposes to collect and store photographs of physical or anatomical features such as scars, skin marks, and tattoos. Many immigrants come to the United States fleeing their home country where persecution may have led to physical attributes that show the violence they have suffered. It can be traumatic to have these physical scars exposed and photographed. Physicians for Human Rights describe analyzing such a wound for an asylum seeker saying, “I sought to ease

⁹⁸ The Home Office, NATIONAL DNA DATABASE ANNUAL REPORT 2012/13, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/252885/NDNAD_Annual_Report_2012-13.pdf.

⁹⁹ Natasha Singer and Cade Metz, *Many Facial-Recognition Systems are Biased, Says U.S. Study*, THE NEW YORK TIMES, (Dec. 19, 2019), www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

¹⁰⁰ *Id.*

¹⁰¹ Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, THE WASHINGTON POST, (July 7, 2019), www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

her vulnerability and avoid re-traumatization.”¹⁰² This kind of compassion is not something that DHS is likely to be able to replicate. Should the changes to their surveillance methods be implemented, photographs of every immigrant’s anatomical features could become a reality—it would become the norm. As such, DHS officers would be desensitized to how they are carrying out their actions and further the trauma that migrants are coming here to escape.

h. DHS Should Withdraw Its Proposal to Collect Palm Prints.

Hygiene will always be an issue regarding those biometric modalities that require direct contact with the technology. Now, during COVID-19, it becomes a matter of life and death. As we have seen, DHS has failed to provide sanitary and safe facilities to immigrants which has already led to COVID being spread among immigrants who are detained.¹⁰³ Immigrants from the Farmville Detention Center in Virginia suffered a COVID-19 outbreak because DHS ignored public health guidance.¹⁰⁴ We cannot be sure that ICE will maintain proper hygiene when administering this test, as it fails to do so already. Adding more modalities of biometrics will increase DHS’ work and will lead to more problems, not fewer.

Further, DHS relies on data and rationale for collecting palm prints that come from criminal investigation.¹⁰⁵ Immigrants applying for benefits should not be subjected to standards set for criminal investigations, and the rationale for expanding biometrics collection should not be derived from criminal justice sources. Immigrants applying for benefits should not be treated like criminals or be evaluated from a criminal justice-oriented framework. DHS should use the methods that are most minimally invasive that establish the information necessary to grant the benefit. When establishing an immigrant’s identity, officers are comparing fingerprints to those previously taken for travel purposes, not to partial prints at crime scenes. There is no indication that in the context of establishing an immigrant’s identity that a palm print would add significant informational value.

i. DHS Should Withdraw Its Proposal to Implement Iris Scanning Technology.

DHS’ proposal to record and maintain a database of iris scans should be withdrawn, as it is a significantly higher risk than other modalities of biometrics in the event of data breaches. The implications of a database with tens of millions of iris scans is chilling; as the Electronic Frontier Foundation has noted, a database of iris scans “raises serious civil liberties and privacy concerns” as it can “track people without their knowledge or consent” and enable long-range identification.¹⁰⁶ In addition, iris scans are not foolproof, and can yield false negative error rates

¹⁰² Norma Price, MD, *Written in the Scars: How Medical Evidence Debunks Trump’s Border Rhetoric*, Physicians for Human Rights, (June 19, 2019), <https://phr.org/our-work/resources/written-in-the-scars-how-medical-evidence-debunks-trumps-border-rhetoric/>.

¹⁰³ International Rescue Committee, *COVID-19 escalating in ICE detention centers as states hit highest daily records - and ICE deportation flights into Northern Triangle continue*, (Aug. 3, 2020), www.rescue.org/press-release/covid-19-escalating-ice-detention-centers-states-hit-highest-daily-records-and-ice.

¹⁰⁴ Jenny Gathright, *Inspection Finds ‘Systematic’ Failings in Farmville Immigrant Detention Center Response to COVID-19 Outbreak*, WAMU, (Sept. 10, 2020), <https://wamu.org/story/20/09/10/inspection-finds-systematic-failings-in-farmville-immigrant-detention-center-response-to-covid-19-outbreak/>.

¹⁰⁵ 85 FED. REG. at 56355-56.

¹⁰⁶ Electronic Frontier Foundation, *Street-Level Surveillance; Iris Recognition*, www EFF.org/pages/iris-recognition#:~:text=Perhaps%20the%20biggest%20threat%20of,from%20more%20and%20more%20people.

of 2.5 to 20 percent.¹⁰⁷ As noted above, DHS has a history of poor data security practices, and a database of iris scans would be a dangerous tool in the wrong hands.

This modality also could be abused by DHS officers, as immigrants may not even be advised as to what method is being used. By using the term “biometrics,” DHS can just inform immigrants that it is collecting biometric information for their immigration case without disclosing that their retinas are being scanned from a distance.

j. DHS Should Withdraw Its Proposal to Collect Voice Print Data.

DHS’s proposal to collect and retain voice print data should be withdrawn, as it is overly intrusive, and can be inaccurate as voices can change over time. DHS proposes to use voice prints as an identifier and to confirm identities at the call center. Like other biometric identifiers, the storage and use of voice prints implicate privacy concerns. Speech recognition “pierces the veil of anonymity” by linking a disembodied voice to a particular identity; collecting voice prints and later using those for identification purposes can create many of the same concerns related to intrusion of privacy as facial recognition technology.¹⁰⁸ The possibility of both false positive and false negative identifications is particularly worrisome in the use of voice prints, as is the presence of both race and gender bias, which could adversely impact people who speak non-American accented English and people who are transgender, among others.¹⁰⁹ DHS fails to explain why a less intrusive mechanism, such as entry of an A-number or a code, could not be used for telephonic and electronic verification.

k. DHS Should Withdraw the Proposal to Expand Collection of “Biometrics” to Children Under 14 years Old.

CLINIC strongly opposes the proposal to expand biometrics collection to all children, regardless of age—both in the context of applications for benefits and during encounters with ICE or CBP. The proposed rule would also expand biometrics collection to forms where it is not currently required, such as petitions for Special Immigrant Juvenile Status, Form I-360. These unnecessary changes frustrate Congress’s intent in providing humanitarian protections to vulnerable children, gravely infringe on children’s privacy interests, and risk trauma and harm to already vulnerable children.

¹⁰⁷ Alice Lipowicz, *NIST Tests Accuracy in Iris Recognition for Identification*, FEDERAL COMPUTER WEEK, (Apr. 23, 2012), <https://fcw.com/articles/2012/04/23/nist-iris-recognition.aspx>.

¹⁰⁸ Oleksandr Pastukhov and Els Kindt, *Voice Recognition: Risks to Our Privacy*, FORBES, (Oct. 6, 2016), www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/#15581a52786d.

¹⁰⁹ Joan Palmiter Bajorek, *Voice Recognition Still Has Significant Race and Gender Biases*, HARVARD BUSINESS REVIEW, (May 10, 2019), <https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases>.

i. The proposed rule's elimination of a minimum age threshold for biometrics collection on children is contrary to congressional intent.

Where Congress has spoken about the need for DHS to collect biometrics on children, it has clearly provided the age of 14 as the minimum age for such collection.¹¹⁰ The proposed rule ignores these carefully constructed minimum age thresholds and the attendant sensitivity these statutes show toward children under 14. Instead, the rule authorizes DHS to engage in widespread and routine biometrics collection—including DNA, fingerprints, facial image, iris image, and voiceprints—on children of all ages, even babies.

The rule's proposal to collect sensitive biometrics information from children regardless of age is also contrary to the purpose behind the Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA), which enacted provisions designed to protect vulnerable unaccompanied children and address their specialized needs.¹¹¹ Instead of following Congress's mandate to enact regulations regarding the processing of unaccompanied children's immigration relief applications which "take into account the specialized needs of unaccompanied alien children" and "address both procedural and substantive aspects of handling unaccompanied alien children's cases,"¹¹² the proposed rule will cause unnecessary and unconsidered harm to unaccompanied children, as described below.

ii. The proposed rule would gravely infringe on children's privacy interests.

The right to privacy is a fundamental right, enshrined in U.S. constitution and recognized in Article 12 of the Universal Declaration of Human Rights and Article 16 of the U.N. Convention on the Rights of the Child.¹¹³ The heightened importance of protecting children's privacy interests is a broadly recognized principle reflected across federal legislation and policies.¹¹⁴

The proposed rule's intent to broadly collect and share identity data on young children raises serious privacy concerns. Under the rule's broad biometrics collection regime, DHS would collect and store massive amounts of personal data on every child it encounters, no matter how young. The proposed rule does not meaningfully engage with privacy implications, merely noting that there "could be some unquantified impacts related to privacy concerns for risks associated with the collection and retention of biometric information" and that "this rule would expand the population that could have privacy concerns."¹¹⁵ DHS does not address at all the

¹¹⁰ See INA §§ 287(f)(1) ([T]he Commissioner shall provide for the fingerprinting and photographing of each alien 14 years of age or older against whom a proceeding is commenced under section 1229a of this title."); Sec. 262(a) ("It shall be the duty of every alien now or hereafter in the United States, who . . . is fourteen years of age or older . . . to apply for registration and to be fingerprinted. . .").

¹¹¹ See TVPRA § 235, Pub. L. 110-457, 122 Stat. 5044.

¹¹² *Id.* § 235(d)(8).

¹¹³ U.N. General Assembly, *Universal Declaration of Human Rights* (Dec. 10, 1948), www.un.org/en/universal-declaration-human-rights/; U.N. General Assembly, *Convention on the Rights of the Child*, (Nov. 20, 1989), www.ohchr.org/en/professionalinterest/pages/crc.aspx.

¹¹⁴ See, e.g., Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99.

¹¹⁵ 85 FED. REG. at 56343.

privacy impacts and costs of the proposal specific to children. This intrusion on children's privacy interests is unwarranted.

Not only does the proposed rule confer expansive authority on DHS to collect and store children's biometric data, but it also authorizes DHS to share this information "with appropriate federal, state, and local law enforcement; or intelligence community entities; foreign governments, as authorized by law and/ or international agreements."¹¹⁶ This expansive authority to share private data of children is unfounded and goes far beyond any legitimate purpose behind USCIS collection of biometrics for purposes of adjudication of benefits. Further, while granting DHS broad authority to collect and share biometric data, the rule does not incorporate statutory confidentiality mandates that DHS is obligated to follow and that protect certain vulnerable populations.¹¹⁷ The NPRM's explanation for why it does not codify those statutory protections is unintelligible.¹¹⁸

The proposal to collect, store, and share biometric data on children of all ages is particularly inappropriate given young children's inability, due to age, to give informed consent to such practices.¹¹⁹ Congress has highlighted the need for recognizing and respecting the informed consent of children. A Majority Staff Report of the Senate Committee on Homeland Security and Governmental Affairs issued on January 11, 2019 and entitled "How the U.S. Immigration System Encourages Child Marriages" is persuasive in its logic.¹²⁰ The report notes that neither USCIS nor the Department of State requires a showing of consent to marry from either the petitioner or the noncitizen beneficiary when adjudicating I-130 or I-129F petitions. It details how USCIS approved the I-130 petition for a spousal immigration benefit for the forced marriage between a U.S. citizen and 13-year old child marriage victim who subsequently suffered physical and sexual abuse during the marriage. The report assesses that she "is just one of the thousands of U.S. women and girls forced into a child marriage involving the U.S. immigration system" and that these forced marriages are predicated upon a lack of informed consent from minors.¹²¹

This congressional report highlights the damaging unintended consequences that result from a system where no guardrails are in place for the government to ensure that its actions do not result in abuse of the child—in this case, on the topic of forced marriage. Similarly, a blanket requirement subjecting children under 14 to biometrics collection where they are similarly unable to comprehend the consequences of the decision they are making is likely to result in similar unintended consequences and potential abusive results. DHS should respect Congress's

¹¹⁶ Proposed 8 CFR § 103.16(d); 85 FED. REG. 56352 (stating that "DHS plans to use the biometric information collected from children for identity management in the immigration lifecycle only, but will retain the authority for other uses in its discretion" and that USCIS may share biometrics, including DNA test results and partial DNA profiles, "with other agencies").

¹¹⁷ See 8 U.S.C. § 1367.

¹¹⁸ 85 FED. REG. at 56350.

¹¹⁹ Other DHS biometrics-based initiatives recognize the need for parental consent for children under the age of 18. See, e.g., CBP, Global Entry Eligibility, Children, www.cbp.gov/travel/trusted-traveler-programs/global-entry/eligibility/children (last modified Jan. 25, 2017).

¹²⁰ United States Senate Committee on Homeland Security and Governmental Affairs, *How the U.S. Immigration System Encourages Child Marriages* (Jan. 11, 2019), www.hsgac.senate.gov/imo/media/doc/Child%20Marriage%20staff%20report%201%209%202019%20EMBARGOED.pdf.

¹²¹ *Id.* at 3.

concerns for the lack of consent for children in the U.S. immigration system and withdraw this proposed rule that signals to immigrant children that they do not have consent or ownership over their bodies.

iii. The proposed rule exposes children to unwarranted, lifelong data security risks.

By collecting, storing, and sharing a vast amount of data on children, the proposed rule exposes them to lifelong security risks. The NPRM simply remarks that “data security is an intangible cost, and we do not rule out the possibility that there are costs that cannot be monetized that accrue to aspects of privacy and data security.”¹²² Nowhere does it meaningfully engage with the grave data security concerns implicated by expansive collection of biometric data on children. The “misuse of children’s biometric information can have permanent and serious consequences, especially in terms of privacy and identity fraud.”¹²³ Children have an increased likelihood of being exposed to “lifelong data risks,” and as “more data will be collected on children over their lifetime than ever before, . . . the future use, applications and impact of this data on their lives is unpredictable.”¹²⁴ Further, unlike a password, biometric data cannot be changed if it is subject to a breach.

Indeed, DHS has a history of mishandling the sensitive biometric data it collects. The DHS Office of Inspector General recently issued a report finding that CBP “did not adequately safeguard” sensitive biometric data gathered through a facial recognition program, resulting in a serious data breach that compromised “approximately 184,000 traveler images from CBP’s facial recognition pilot; at least 19 of the images were posted to the dark web.”¹²⁵

iv. The proposal to expand collection of biometric data on children raises serious risks of error.

The proposed expanded collection of biometric data on children is also inappropriate because of the increased risk of error in matching young children’s biometric data.¹²⁶ Even DHS officials

¹²² 85 FED. REG. at 56388.

¹²³ UNICEF, *Faces, Fingerprints, and Feet*, at 19 (July 2019), available at <https://data.unicef.org/resources/biometrics/> [hereinafter “UNICEF REPORT”].

¹²⁴ *Id.*

¹²⁵ Office of Inspector General, U.S. Department of Homeland Security, *Review of CBP’s Major Cybersecurity Incident During a 2019 Biometric Pilot*, OIG 20-71, at 5-6 (Sept. 21, 2020), www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

¹²⁶ UNICEF REPORT, *supra* note 143, at 16 (noting that “failures or errors are more likely to occur in children”); *id.* at 19 (“Biometric systems have primarily been designed to work with adults, and as such, the technology is not always appropriate for use in recognizing children. This may be due to the difficulty in capturing the biometric trait (such as an iris scan with very young children); the relatively poor performance of the trait among certain age groups (facial recognition); or the low levels of user acceptance (DNA.)”); *see also* U.S. Dep’t of Commerce, Nat’l Inst. Standards & Technology, *Face Recognition Vendor Test Part 3: Demographic Effects*, at 2 (Dec. 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (“We found elevated false positives in the elderly and in children; the effects were larger in the oldest adults and youngest children, and smallest in middle aged adults.”); *id.* at 15 (“[I]t is possible that certain demographics yield photographs ill-suited to face recognition e.g. young children . . .”).

have recognized the inaccuracy of matching young children’s biometric data.¹²⁷ The proposed rule would collect data regarding physical characteristics such as facial image and voice print, characteristics that will inevitably change as a child matures to adulthood. DHS’s plan to use the biometric data “to ensure the immigration records created for children can be related to their adult records later,”¹²⁸ is problematic given the likelihood of inaccurate and erroneous matching. This in turn creates a risk that a child will end up being falsely accused of a crime in the future based on biometrics DHS collected on them at a very young age. This risk is compounded given the higher rates of inaccuracy of technology such as face recognition among not only children but also people of color. Indeed, one government study from 2019 revealed that Asian and African American people were up to 100 times more likely to be misidentified than white people, and Native Americans had similarly high rates of false positives.¹²⁹ Immigrant children of color will be especially susceptible to false positives, based on the results of this study. Further, a recent government study revealed that facial recognition systems are even more inaccurate during the current era of COVID-19 and widespread mask wearing to protect public health—facial recognition technology had error rates between five and 50 percent in matching digitally applied face masks with photos of the same person without a mask.¹³⁰

v. The proposal to collect biometrics from young children would be unduly physically intrusive and cause unnecessary mental trauma.

DHS’s proposal to collect biometrics on young children does not take into account the logistical difficulties such collection will entail. The NPRM says that collection of “the biometrics of all minors during their initial immigration enforcement processing . . . will require some operational changes for agents in the field.”¹³¹ But it does not explain how it intends for agents to physically collect this information from small children. It will inevitably involve forceful touch, with babies and toddlers likely squirming and crying as an agent restrains them to collect their fingerprints, photographs, and other biometrics. Infants and young children will not be able to understand what is happening and the physical act of collection has the likelihood to cause distress and mental trauma. Even for children who do have some understanding of what fingerprinting is,

¹²⁷ See Geneva Sands, *US Border Patrol Begins Fingerprinting Children Under 14 Years Old*, CNN, Apr. 24, 2019, www.cnn.com/2019/04/24/politics/us-border-patrol-fingerprinting-children-new-policy/index.html (“From a technical perspective, the reason Customs and Border Protection previously did not fingerprint children until they turned 14 is ‘because your fingerprint doesn’t solidify until that time,’ said a former DHS official, who worked on immigration policy and biometrics. Fingerprint algorithms rely on features that are consistent only after 14 years of age, said the former official.”); see also 85 FED. REG. 56357 (recognizing that children’s “physical appearances can change relatively rapidly”); 85 Fed. Reg. at 56351 (“DHS recognizes that biometric reuse is acceptable, when there is identity verification, but in the case of children biometric reuse could be impacted by the rapidly changing physical attributes of children.”).

¹²⁸ 85 FED. REG. 56340.

¹²⁹ National Institute of Standards and Technology, *NIST Study Evaluates Effects of Race, Age Sex on Face Recognition Software* (Dec. 19, 2019), www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; see also Amnesty International, *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance* (June 11, 2020), www.amnestyusa.org/wp-content/uploads/2020/06/061120_Public-Statement-Amnesty-International-Calls-for-Ban-on-the-Use-of-Facial-Recognition-Technology-for-Mass-Surveillance.pdf.

¹³⁰ National Institute of Standards and Technology, *NIST Launches Studies into Masks’ Effect on Face Recognition Software* (July 27, 2020), www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software.

¹³¹ 85 FED. REG. at 56386.

from the perspective of a young and unaccompanied child, being subjected to this intrusive process is likely to cause or exacerbate trauma.¹³²

Even assuming it were theoretically possible to collect biometrics from babies and young children without trauma or harm, DHS officers do not have the training or expertise to perform collections on small children without causing pain or trauma. The fact that DHS does not intend to provide adequate training to its officers regarding collection of biometrics on young children is evident from its statement that it anticipates the training it intends to provide on biometrics collection of children will take a mere hour of employees' time.¹³³ The proposal nowhere acknowledges DHS's duty to "provide specialized training to all Federal personnel . . . who have substantive contact with unaccompanied alien children."¹³⁴ In reality, subjecting young children to forced biometrics collection by DHS agents thwarts the TVPRA's purpose to protect unaccompanied children and address their specialized needs.

vi. DHS has not shown how the collection of biometric data of children under 14 solves an identified problem.

In attempting to justify the proposed expansion of biometrics collection to children under 14, the proposed rule repeatedly cites combatting human trafficking,¹³⁵ however, it offers no data or evidence that suggest that biometrics collection on young children would actually combat trafficking.¹³⁶ Children often arrive in the United States with non-biological parent caregivers or guardians, and the lack of a genetic parent-child relationship is not determinative of trafficking. The proposed rule does not consider less intrusive and more accurate alternatives to identify trafficking of children.

The proposed rule also justifies expanding biometrics collection to young children in order to "confirm[] the absence of criminal history or associations with terrorist organizations or gang membership"¹³⁷ and to combat identity fraud such as instances where an adult is posing as a child.¹³⁸ Again, DHS provides no evidence or data to confirm that these are widespread problems that would call for such an expansive and problematic surveillance program. DHS provides no statistics about the number of children under the age of 14 who have a documented criminal history that biometrics collection would reveal. Nor does DHS provide data or evidence that

¹³² Cf. Elaine Chase, Agency and Silence: *Young People Seeking Asylum Alone in the UK*, 40 BRITISH JOURNAL OF SOCIAL WORK 2050, 2052 (2010), www.dentalage.co.uk/wp-content/uploads/2014/09/chase_e_2010_brit_j_soc_work.pdf ("Within the context of asylum-seeking, many young people described themselves as being under regular scrutiny. Such scrutiny was multi-faceted, being variably exercised by social care professionals, immigration officials, other statutory sector personnel, as well as by the media and the general public. Within these arrangements, young people find different ways of engaging with the 'omnipotence' of the surveillance and strive to make sense of the structures through which they are channelled.").

¹³³ 85 FED. REG. at 56387.

¹³⁴ TVPRA § 235(e).

¹³⁵ See, e.g., 85 FED. REG. at 56365-66, 56368, 56386-87.

¹³⁶ The NPRM contains this confusing hypothetical statement, with no data or evidence as to the frequency of this type of problem and how biometrics collection would solve it: "For example, a vulnerable child with similar biographical characteristics to a child who has lawful immigration status in the United States may be moved across the border under the assumed identity of that other child, although DHS does not have specific data to identify the entire scope of this problem." 85 FED. REG. 85.

¹³⁷ 85 FED. REG. at 56340.

¹³⁸ 85 FED. REG. at 56352.

adults posing as children under 14 is a significant or widespread problem that biometrics collection would resolve.

Instead, the real purpose of the proposed rule appears to be to treat immigrant children of color like criminals. The children may interpret the government's efforts to continuously obtain information about them as a sign that the government does not trust them and that the government expects them to do wrong, to break the law. The proposal would treat young children no differently than adults—subjecting them, no matter how young, to fingerprinting and other forensic evidence-gathering processes. This reality thwarts the humanitarian and child-sensitive purpose of the TVPRA. For the reasons discussed above, DHS should abandon its proposal to collect biometrics on children under 14.

I. The Collection of Biometrics of Children Under 14 Years Old Will Subject Vulnerable Children to False Gang Allegations Rather Than Protecting Them from Gangs.

DHS justifies applying biometrics collection to children under 14 by claiming that this expansion will “increase the U.S. Government’s capabilities of determining the identity of a child who may be vulnerable to *gang affiliation*,”¹³⁹ and “ensure the immigration records created for children can be related to their adult records later, [...], while confirming the absence of criminal history or associations with terrorist organizations or *gang membership*.” However, at no point does DHS define the terms “gang,” “gang affiliation,” or “gang membership.”¹⁴⁰ DHS further fails to explain why and how immigrant children and youth are vulnerable to gang affiliation or membership in the first place, nor does DHS explain how it intends to use any information on “gang affiliation” to protect vulnerable children. In fact, DHS also fails to contemplate assurances as to how this proposal would not ensnare immigrant children in false gang allegations that will lead to their swift removal from the United States without due process. Indeed, this NPRM would substantially increase the criminalization of immigrant youth and fearmongering around immigrants overall.

- i. DHS employs “gang membership” and “gang affiliation” without defining these terms or considering the legal implications and consequences of these terms.*

DHS’s failure to define “gang,” “gang affiliation,” and “gang membership” acknowledges the longstanding problems with the legal significance and application of these terms. Courts have defined “member” or “membership” as “meaning that a person bears a relationship to an organization that is not accidental, artificial or unconsciously in appearance only.”¹⁴¹ No definition of “gang affiliation” exists¹⁴² and the term often seems to be used interchangeably with “gang membership.”¹⁴³ Law enforcement agencies lack consensus on a uniform definition of a

¹³⁹ 85 FED. REG. at 56364.

¹⁴⁰ 85 FED. REG. at 56340.

¹⁴¹ *Galvan v. Press*, 347 U.S. 522, 528 (1954).

¹⁴² Federal law, states’ laws, and the INA are all devoid of a definition for gang affiliate.

¹⁴³ See, e.g., *Goree v. State*, 748 So. 2d 829, 837 (Miss. Ct. App. 1999) (using “gang affiliation” and “gang membership” interchangeably); See also Laila L. Hlass and Rachel Prandini, *Deportation by Any Means Necessary*, Immigrant Legal Resource Center, at 6, www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-

“gang.”¹⁴⁴ In fact, when states have attempted to define “gang,” these laws have faced First Amendment freedom of association and Fourteenth Amendment “void for vagueness” challenges. For example, when New Jersey tried to impose criminal penalties via legislation for mere membership in a gang without any unlawful act or omission, it tried to define “gang.”¹⁴⁵ The statute defined a gang merely by the phrase “consisting of two or more persons,” a term so vague that persons of ordinary intelligence would necessarily have to guess at its meaning and application, because the statute brought within its range any noncriminal association or group.¹⁴⁶ The U.S. Supreme Court invalidated that New Jersey anti-gang statute as unconstitutionally vague.¹⁴⁷

Since the Supreme Court’s *Lanzetta v. State of New Jersey* decision in 1939, states seeking to punish illegal activity more harshly if there is a “gang” component have grappled with defining “gang” in a manner consistent with the First Amendment and *Lanzetta*. For example, subdivision (f) of section 186.22 of the California Penal Code prohibits membership in a “criminal street gang,” defined as “any ongoing organization, association, or group of three or more persons, whether formal or informal, having as one of its primary activities the commission of one or more of the criminal acts enumerated in paragraphs (1) to (8), inclusive, of subdivision (e), which has a common name or common identifying sign or symbol, whose members individually or collectively engage in or have engaged in a pattern of criminal gang activity.” The California legislature specifically declared that this provision was not intended to interfere with the constitutionally protected rights of association and freedom of expression and, indeed, this definition has withstood legal challenges because it is defined specifically, and “its application requires proof of multiple elements.”¹⁴⁸

One of these requirements, found at subdivision (a) of section 186.22 of the California Penal Code, is proof of being an active gang member or participant.¹⁴⁹ In California, “it has been held that a ‘member’ may not be subjected to criminal liability for the acts of the association to which he is a member unless his membership is ‘active,’ a term which has been held to be well understood in common parlance.”¹⁵⁰ By using the phrase “actively participates,” the California Legislature sought to prevent prosecution of persons who were no more than nominal or inactive

[20180521.pdf](#) (“[I]n 17 [of 40 reported] cases, [clients] were accused of being both a gang member and an associate.”).

¹⁴⁴ See National Gang Center, NATIONAL YOUTH GANG SURVEY ANALYSIS, www.nationalgangcenter.gov/Survey-Analysis (last visited Oct. 5, 2020) (“There is no widely or universally accepted definition of a ‘gang’ among law enforcement agencies.”); C. Ronald Huff, *Preface* to GANGS: THE ORIGINS AND IMPACT OF CONTEMPORARY YOUTH GANGS IN THE UNITED STATES, vii (Scott Cummings & Daniel J. Monti eds., 1993) (noting that no comprehensive definition of “gang” has been put forward).

¹⁴⁵ *Lanzetta v. State of New Jersey*, 306 U.S. 451, 458 (1939).

¹⁴⁶ *Id.* at 453, 457.

¹⁴⁷ *Id.*

¹⁴⁸ *In re Nathaniel C.*, 228 Cal. App. 3d 990, 1000 (Ct. App. 1991).

¹⁴⁹ “Any person who actively participates in any criminal street gang with knowledge that its members engage in or have engaged in a pattern of criminal gang activity, and who willfully promotes, furthers, or assists in any felonious criminal conduct by members of that gang, shall be punished by imprisonment in a county jail for a period not to exceed one year, or by imprisonment in the state prison for 16 months, or two or three years.” (Italics added.). CAL. PENAL CODE § 186.22 (West).

¹⁵⁰ *People v. Green*, 227 Cal. App. 3d 692, 699-700 (Ct. App. 1991) (citing *Scales v. United States*, 367 U.S. 203, 223 (1961)).

members of a criminal street gang.¹⁵¹ Therefore, the court in *Green* found the terms “actively participates,” “member,” “membership,” “criminal street gang,” “knowledge,” “pattern of criminal gang activity,” and “willfully promotes, furthers, or assists” to be sufficiently certain to give a defendant “reasonable notice of the conduct which [the statute] prohibits and is no more susceptible to arbitrary enforcement than any other criminal statute.”¹⁵² Similarly, federal courts have held that evidence of gang membership is inadmissible unless the evidence is sufficient to establish that the defendant is a member of the group, the group’s aims are illegal, and the defendant intended to further those illegal aims.¹⁵³ Therefore, while the right of association may be limited, it is only limited upon a clear showing that an association or organization is actively engaged in lawless conduct,¹⁵⁴ and by a prosecutor proving that the person is an active member or participant.

While there are limitations to the application of anti-gang or sentencing enhancement laws, these laws have faced criticism for allowing prosecutors to cast too wide of a net. This is because these laws allow prosecutors to introduce gang enhancements at sentencing to make a weak case strong through “potentially inflammatory information that might otherwise be legally irrelevant.”¹⁵⁵ Examples of such irrelevant information could include race or ethnicity, place of residence, a connection to a name or symbol, or a family relationship. According to the California Department of Corrections and Rehabilitation, “Black and Latino inmates account for more than 90 percent of inmates with gang enhancements; fewer than 3 percent are white.”¹⁵⁶ Youth advocates allege these laws allow for the penalization of youth of color for environmental factors outside of their control. Furthermore, these laws arguably criminalize youth based on their choices of pop culture style or wearing a particular color because of a personal preference or because their parents purchased the item without knowing the color’s connection to a gang. In essence, anti-gang or sentencing enhancement laws allow states to punish illegal activity more harshly if there is merely “gang affiliation” as opposed to “gang membership.”¹⁵⁷

Despite the lengthy jurisprudential history analyzing the definition of “gang” and sensitive constitutional issues that arise in defining and applying anti-gang laws, DHS nonetheless resorts to using the general terms “gang membership” and “gang affiliation” without any definition or explanation. While it is unclear what DHS means by the term “gang affiliation,” it is clear that this label and the broad criteria this label has traditionally encompassed have led to severe and unfair consequences when prosecutors apply gang enhancement laws.

¹⁵¹ *Id.* at 700.

¹⁵² *In re Alberto R.*, 235 Cal. App. 3d 1309, 1319 (Ct. App. 1991).

¹⁵³ *United States v. Lemon*, 723 F.2d 922, 941 (D.C. Cir. 1983).

¹⁵⁴ *See Dennis v. United States*, 341 U.S. 494, 516–517 (1951).

¹⁵⁵ Daniel Alarcón, *How Do You Define a Gang Member?*, THE NEW YORK TIMES MAGAZINE, (May 27, 2015), www.nytimes.com/2015/05/31/magazine/how-do-you-define-a-gang-member.html.

¹⁵⁶ *Id.*

¹⁵⁷ George Khoury, *Gang Affiliation Charges: Is Gang Affiliation a Crime?*, FINDLAW, (Oct. 14, 2016), <https://blogs.findlaw.com/blotter/2016/10/gang-affiliation-charges-is-gang-affiliation-a-crime.html>.

- ii. *DHS offers no explanation or data for why immigration children under 14 may be vulnerable to gang affiliation or gang membership and no plans for how DHS will respond if it identifies any children as such.*

Despite the absence in the NPRM of a definition for “gang membership” or “gang affiliation” and the controversy surrounding the application of these labels, DHS nonetheless justifies applying biometrics collection to children under 14 so that it can identify children who may be vulnerable to gang affiliation and to disconfirm evidence of gang membership. However, DHS fails to explain how biometrics will flag “gang affiliation” and “gang membership” markers and why it is important to identify this group of children for these markers.¹⁵⁸ Further, DHS fails to offer any evidence to support its assumption that immigrant children under 14 are either currently affiliated with gangs or are likely to become gang members in the future. The logical inference of this is that DHS began with its conclusion and has not even bothered to articulate how the agency arrived at this destination.

Since DHS failed to explain or show any data to justify how it arrived at this conclusion, the public can only speculate as to what DHS’s rationale or data might be, if any exists. Accordingly, we shall offer some hypotheses. Perhaps DHS believes that immigrant children because of their race or ethnicity are more likely to be affiliated with gangs currently or will become gang members in the future? Perhaps DHS believes that immigrant children are currently connected to gangs via family members?

Additionally, one wonders what criteria DHS might use to determine current gang affiliation and, if that criteria is overbroad and includes factors outside of their control, might this not lead to DHS identifying most children as gang affiliates? For example, imagine a circumstance where a child was targeted by gangs in the country they fled. Would this targeting suffice as a “gang affiliation” hit? Perhaps DHS thinks that immigrant children may be more likely to become gang members in the future based on where they live? Or, perhaps DHS realizes that treating immigrant children as criminals by signaling that they must give up more privacy than anyone else via required biometrics checks has the potential of serving as a self-fulfilling prophecy? Or, maybe, DHS understands that continuously making immigrant children feel like “the other” their entire lives despite them obtaining U.S. citizenship may increase the chances of immigrant children joining a gang at some point in their lives? While this level of speculation by the public might be deemed harsh, it is no harsher than what DHS attempts to do via this NPRM: to designate immigration children as criminal simply because of their immigrant status. Regardless, by failing to show its work, DHS invites nothing but speculation into its motives.

Whatever DHS’s justifications for wanting to identify children who may be vulnerable to gang affiliation and confirm a lack of gang membership may or may not be, DHS also fails to explain how identifying any immigration children as gang affiliates or gang members now or in the future will help to protect these children. Again, DHS’s silence on its reasoning does nothing but invite the public to speculate further. For example, does DHS plan to fund programs that will protect children from gangs? Will DHS work with local law enforcement to ensure that the prosecution of any criminal charges that arise from gang affiliation or membership do not lead to

¹⁵⁸ Tal Kopan, *MS13 is Trump’s Public Enemy No. 1, but should it be?*, CNN POLITICS, (Apr. 29, 2017), <https://www.cnn.com/2017/04/28/politics/ms13-explained-immigration-sessions/index.html>.

sentencing enhancement? Or, will DHS instruct ICE Enforcement and Removal Operations to not pursue the removal of those whose biometrics flag these vulnerabilities?

No one knows what the future holds for immigrant children, but offering them support and resources seem like wise investments aimed at ensuring they thrive and succeed. Conversely, subjecting them to more government control when they have engaged in no wrongdoing sends the opposite message and furthers the myth that children are likely to engage in criminal conduct by virtue of the fact that they are immigrants of color.¹⁵⁹ However, if DHS does have plans to identify these vulnerable children in order to better support them, CLINIC welcomes that and looks forward to them sharing their plan.

iii. Subjecting children under 14 to biometrics will lead to an increase in false allegations of gang affiliation, as shown by recent and ongoing DHS practice.

Instead of protecting immigrant children from gang affiliation or gang membership, seeking their biometrics information will only serve to add them to gang databases that DHS could then rely on to argue for their removal from the United States.

Since DHS fails to define “gang membership” and “gang affiliation” and also fails to explain how biometrics will aid in identifying these children, the public must again engage in speculation. And based on present practices, the public should assume that DHS will enter biometrics into a set of databases shared across state governments and federal government agencies, which have long served as a source of gang allegations against noncitizens.¹⁶⁰ Commonly used databases include the privately owned GangNET, the FBI’s National Crime Information Center, and local and state versions such as California’s CalGang and Chicago’s CLEAR Data Warehouse. These databases include personal details such as addresses, identifying physical characteristics, photographs, nationality, and alleged affiliation with or role in a gang, among other information.

How accurate these databases are is an important question to ask. A report by the California state auditor released last year found that the state database, known as CalGang, was rife with inaccuracies, included many people without enough evidence of their supposed gang ties, and might violate their privacy rights.¹⁶¹ Of the roughly 150,000 people in the CalGang database, 21 percent are black and 61 percent are Latino, according to the state report.¹⁶² Erroneous additions

¹⁵⁹ Alex Nowrasteh, *Criminal Immigrants in Texas in 2017: Illegal Immigrant Conviction Rates and Arrest Rates for Homicide, Sex Crimes, Larceny, and Other Crimes*, IMMIGRATION RESEARCH AND POLICY BRIEF NO. 13, CATO Institute, (Aug. 27, 2019), www.cato.org/publications/immigration-research-policy-brief/criminal-immigrants-texas-2017-illegal-immigrant; www.themarshallproject.org/2019/05/13/is-there-a-connection-between-undocumented-immigrants-and-crime.

¹⁶⁰ ICE GANGS DATABASE: DATA ENTRY AND USE, *ICE Policy System*, (2017), www.documentcloud.org/documents/3467677-ICEGang-Classification-Policy.html.

¹⁶¹ California State Auditor, *THE CALGANG CRIMINAL INTELLIGENCE SYSTEM: AS THE RESULT OF ITS WEAK OVERSIGHT STRUCTURE, IT CONTAINS QUESTIONABLE INFORMATION THAT MAY VIOLATE INDIVIDUALS’ PRIVACY RIGHTS*, Report 2015-130, California State Auditor, (Aug. 11, 2016), www.auditor.ca.gov/pdfs/reports/2015-130.pdf.

¹⁶² *Id.*

to gang databases have been known to occur due to local law enforcement agency fabricating information or being overzealous.¹⁶³ Seeking removal from gang databases is a long and difficult process; and while in California, for example, the law has changed to provide timely notice of being included in the database and a process to seek removal from the database, neither DHS nor an immigration judge will await the conclusion of this process to proceed with removal proceedings in immigration court.

DHS has fabricated gang allegations, as well. For example, DACA recipient Daniel Ramirez Medina was almost deported after ICE detained him and stripped him of his status because of his tattoo. U.S. District Judge Ricardo S. Martinez, a George W. Bush appointee, ruled that ICE violated procedural due process, and chastised ICE for making “the continued assertion that Mr. Ramirez [Medina] is gang-affiliated, despite providing no evidence specific to Mr. Ramirez [Medina] to the Immigration Court in connection with his administrative proceedings, and offering no evidence to this Court to support its assertions four months later.”¹⁶⁴ Mr. Ramirez Medina was lucky to have had legal counsel to fight this false gang allegation in federal district court where there is a robust adversarial process, due process, and the opportunity for discovery, unlike in immigration court. Indeed, since immigration proceedings are not subject to the same evidentiary standards as are required in the criminal context, DHS seems to exploit these lax standards by using gang allegations with little or no evidence to detain, initiate removal proceedings against, and argue against bond or relief from removal.¹⁶⁵ Furthermore, ICE’s own policy for gang documentation explicitly instructs ICE to keep all mention of gang databases or gang intelligence collection out of court documents resulting in ICE issuing gang allegations during the removal process while hiding behind the policy as a reason why it cannot offer proof of or a basis for the allegation.¹⁶⁶ ICE’s broad immunity from lawsuits¹⁶⁷ coupled with DHS’s lack of transparency allows DHS to allege gang ties in an increasingly politicized immigration court that offers no opportunity for noncitizens to defend themselves, especially if they are *pro se*. This results in railroading and removing noncitizens from the United States with no oversight.

Moreover, ICE’s “Operation Matador” in Suffolk County, New York serves as a recent example of the destruction that information sharing among police departments, ICE, and schools can have on the lives of immigrant youth. Through that operation, ICE arrested approximately 170 unaccompanied children because the Suffolk County Police Department had flagged them as supposed gang members via police officers posted inside schools—known as school resource

¹⁶³ Heather Murphy, *Los Angeles Officers Suspended After Boy Is Wrongly Labeled a Gang Member: A mother’s concerns unleashed an investigation into whether an elite police unit was falsifying records*, THE NEW YORK TIMES, (Jan. 8, 2020), www.nytimes.com/2020/01/08/us/lapd-gang-database.html.

¹⁶⁴ Mark Joseph Stern, *Bad Liars: ICE claimed a Dreamer was “gang-affiliated” and tried to deport him. A federal judge ruled that ICE was lying*, SLATE, (May 16, 2018), <https://slate.com/news-and-politics/2018/05/federal-judge-accused-ice-of-making-up-evidence-to-prove-that-dreamer-was-gang-affiliated.html>.

¹⁶⁵ See New York Immigration Coalition, *SWEPT UP IN THE SWEEP: THE IMPACT OF GANG ALLEGATIONS ON IMMIGRANT NEW YORKERS*, (May 2018), http://thenyic.pi.bypronto.com/wp-content/uploads/sites/2/2018/06/SweptUp_Report_Final-1.pdf; CLINIC, *The University of Maryland Carey School of Law Immigration Clinic, and Maryland Immigrant Rights Coalition’s (MIRC), PRESUMED DANGEROUS: BOND, REPRESENTATION, AND DETENTION IN THE BALTIMORE IMMIGRATION COURT*, (2019), <https://cliniclegal.org/resources/enforcement-and-detention/presumed-dangerous-bond-representation-and-detention-baltimore>.

¹⁶⁶ *Ibid*, ICE GANGS DATABASE: DATA ENTRY AND USE, <https://www.documentcloud.org/documents/3467677-ICEGang-Classification-Policy.html>.

¹⁶⁷ See, e.g., *Ziglar v. Abbasi*, 582 U.S. ___ (2017).

officers (SROs). Those SROs collected information and tips that they then passed on to ICE. These SROs were trained to look for items like plastic rosaries, blue bandannas, anything with horns and the numbers 504 and 503, written in notebooks or on hands.¹⁶⁸ Pop culture style items such as black Nike Cortez sneakers and a Brooklyn Nets hat were also on the list.¹⁶⁹ When asked about the process for reporting gang allegations, a Suffolk County SRO said, “It’s submitted, and then I don’t know how it’s disseminated from there. We enter it on a computer, and then it goes to whoever wants to read it within the department.”

Given the known unreliability of gang allegations information in gang databases—whether stemming from local law enforcement, DHS, or SROs—DHS should address how it plans to ensure that the gang allegations against immigrant children are reliable. DHS should also explain how immigrant children now or in the future will be able to challenge the erroneous designation despite not having the right to appointed government counsel in removal proceedings before an immigration judge. Otherwise, recent and ongoing DHS practice—not speculation—has shown us that immigrant children will be criminalized and fast-tracked for deportation based on false and flimsy gang allegations.

III. DHS’S PROPOSAL TO BROADEN THE SCOPE AND DURATION OF ITS SURVEILLANCE IS UNJUSTIFIED AND VAGUE

a. DHS Should Withdraw its Proposal to Conduct Ongoing, “Continuous” Surveillance of U.S. Citizens and of Individuals Who Have Obtained Lawful Status.

DHS currently runs name-based criminal background checks on U.S. citizens and lawful permanent residents petitioning for their immigrant relatives. The proposed rule would allow DHS to obtain and keep the various forms of biometrics to assess criminal history. Just like with most petitions, the individual has to disclose any criminal history. DHS is treating U.S. citizens and lawful permanent residents like criminals in every situation instead of running their search and requesting any missing information where there are gaps. United States citizens and lawful permanent residents should be able to petition for their loved ones without subjecting themselves to a prolonged and in-depth biometrics collection.

CLINIC strongly opposes the proposed rule’s authorization of ongoing surveillance of noncitizens and citizens. The proposed rule would authorize DHS to engage in breathtakingly broad and invasive “continuous immigration vetting” of noncitizens and even naturalized U.S. citizens for an indefinite time after they have obtained lawful immigration status. Under the proposed rule “[a]ny individual alien may be required to submit biometrics again for the purposes of continuous vetting, unless and until he or she is granted U.S. citizenship.”¹⁷⁰ The proposed rule authorizes DHS to require even U.S. citizens to submit to biometrics collection in

¹⁶⁸ Hannah Drier, *How a Crackdown on MS-13 Caught Up Innocent High School Students: The Trump administration went after gang members - and instead destroyed the American dreams of immigrant teenagers around the country*, THE NEW YORK TIME MAGAZINE, (Dec. 27, 2018), www.nytimes.com/2018/12/27/magazine/ms13-deportation-ice.html.

¹⁶⁹ Anjali Tsui, *In Crackdown on MS-13, a New Detention Policy Raises Alarms*, FRONTLINE, (Feb. 18, 2018), www.pbs.org/wgbh/frontline/article/in-crackdown-on-ms-13-a-new-detention-policy-raises-alarms/.

¹⁷⁰ Proposed 8 CFR § 103.16(c)(2).

vague circumstances where the citizen filed “an application” at some point in the past and “the previous approval is relevant” to an unspecified pending application, petition, or benefit request.¹⁷¹

The NPRM justifies this indefinite, continuous vetting as a means to ensure that noncitizens “present no risk of causing harm subsequent to their entry,”¹⁷² but it does not explain how USCIS would evaluate whether an individual meets this standard. Nor does the proposed rule explain how this standard—determining that an individual presents no risk of causing future harm—is relevant to whether an individual was eligible for the benefit they sought and obtained. Indeed, it would be impossible to determine that *any* human being satisfies the standard of presenting “no risk” of causing future harm. Thus, not only is the means (indefinite surveillance) inappropriate, but the ends it seeks to achieve—ensuring that individuals pose no risk of future harm—is impossible.

The indefinite, continuous surveillance regime authorized by this rule poses grave threats to the privacy of foreign-born individuals. It is un-democratic and instead evocative of an authoritarian regime.¹⁷³ It sends a message to the very individuals that the U.S. government has determined are worthy of lawful status in this country that they are suspect and unwelcome. It cultivates an atmosphere of hostility and intimidation that is antithetical to American values, especially freedom, and to CLINIC’s mission to embrace the Gospel value of welcoming the stranger. Finally, by allowing DHS to impose monitoring requirements on individuals with lawful status at its whim, the proposed rule lends itself to racist and discriminatory implementation. DHS has not offered any rationale as to how it would implement this policy in a way that does not target, or disproportionately impact, individuals based on their race or other protected characteristic, as the government has done in previous shameful chapters of American history.¹⁷⁴

DHS currently runs name-based criminal background checks on U.S. citizens and lawful permanent residents petitioning for their immigrant relatives. The proposed rule would allow DHS to obtain and keep the various forms of biometrics to assess criminal history. Just like with most petitions, the individual has to disclose any criminal history. DHS is treating U.S. citizens and lawful permanent residents like criminals in every situation instead of running their search and requesting any missing information where there are gaps. U.S. citizens and LPRs should be

¹⁷¹ *Id.*

¹⁷² 85 FED. REG. at 56340, 56352.

¹⁷³ See, e.g., Paul Mozur & Aaron Krolik, *A Surveillance Net Blankets China’s Cities, Giving Police Vast Powers*, THE NEW YORK TIMES, (Dec. 17, 2019), www.nytimes.com/2019/12/17/technology/china-surveillance.html (“China is ramping up its ability to spy on its nearly 1.4 billion people to new and disturbing levels, giving the world a blueprint for how to build a digital totalitarian state. Chinese authorities are knitting together old and state-of-the-art technologies—phone scanners, facial-recognition cameras, face and fingerprint databases and many others—into sweeping tools for authoritarian control. . . .”); Alina Polyakova & Chris Meserole, *Brookings Institution, Exporting Digital Authoritarianism: the Russian and Chinese Models* (Aug. 27, 2019), www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Nicola Habersetzer, *Human Rights Watch, Moscow Silently Expands Surveillance of Citizens* (Mar. 25, 2020), www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens#.

¹⁷⁴ See, e.g., National Archives, *Japanese-American Internment During World War II*, www.archives.gov/education/lessons/japanese-relocation; Dwight D. Eisenhower Presidential Library, *McCarthyism/The “Red Scare,”* www.eisenhowerlibrary.gov/research/online-documents/mccarthyism-red-scare.

able to petition for their loved ones without subjecting themselves to a prolonged and in-depth biometrics collection.

b. DHS Should Withdraw the Proposal to Require Ongoing, “Continuous” Surveillance of Individuals After They Have Obtained Lawful Status and Until—and Even After—They Have Become U.S. Citizens or Risk Losing That Lawful Status.

CLINIC strongly opposes the proposed rule’s imposition of draconian consequences for missing an appointment. Under the proposed rule, if an individual fails to appear at a scheduled biometrics appointment without “good cause,” DHS “will” deny the pending request and refer the case to immigration court, and “may terminate, rescind, or revoke the individual’s immigration status, petition, benefit, or relief, where authorized by law.”¹⁷⁵ Similarly, if an applicant fails to appear for an interview “without prior authorization from USCIS,” USCIS can deny the benefit or even terminate the individual’s immigration status.¹⁷⁶ The proposed rule does not identify in what scenarios the law would authorize the stripping of someone’s lawful immigration status based on a missed appointment. Coupled with the proposal to conduct “continuous immigration vetting” after an individual has obtained lawful status, the result is an abusive regime where DHS is authorized to continually call an individual in for biometrics, despite them having lawful status and having no pending application, and if the individual fails to appear, DHS may rescind their immigration status and initiate removal proceedings against them. This is a disproportionate and egregiously unfair consequence for missing an appointment, seemingly designed to render more lawful immigrants undocumented.

The unfairness of the proposed consequences for missing an appointment is heightened given the barriers the proposed rule imposes for an applicant to successfully reschedule if they are not able to make the scheduled appointment. The proposed rule authorizes DHS to collect biometrics multiple times,¹⁷⁷ but gives no explanation of why DHS would need to haul someone in multiple times for biometrics collection, particularly given that DHS’s technology allows it to reuse previously collected data.¹⁷⁸ The proposed rule also makes it overly difficult for an individual to reschedule an appointment without risking draconian consequences for failure to appear. Other than allowing one reschedule prior to the biometrics appointment, the regulation only discusses rescheduling “at [DHS’s] discretion” or where, “before issuing the biometrics notice, DHS received a valid change of address request but the biometrics notice was not sent to the updated address.”¹⁷⁹ The rule does not appear to allow for rescheduling for any other reason, such as a car breakdown en route to the appointment, inclement weather, hospitalization, or even a situation where the change of address was in the mail to DHS when DHS issued the notice. In any of these circumstances, the proposed rule would apparently allow DHS to rescind the person’s

¹⁷⁵ Proposed 8 CFR § 103.16(b).

¹⁷⁶ Proposed 8 CFR § 103.2(b)(9)(iv).

¹⁷⁷ Proposed 8 CFR § 103.16(a)(2).

¹⁷⁸ See 85 FED. REG. 56351; USCIS, *Fingerprint Check Update Request: Agreement Between USCIS and ICE* (last updated July 27, 2016), <https://www.uscis.gov/news/alerts/uscis-issues-updates-to-biometrics-collection-guidance> (“[I]n most cases, fingerprint results can be updated with information already available in either an ICE or USCIS system.”).

¹⁷⁹ Proposed 8 CFR § 103.16(a)(7).

immigration status for failure to appear at the biometrics appointment and initiate removal proceedings against them—an absurd, punitive result.

The proposed rule does not take into account or even acknowledge the harmful impact it would have on unaccompanied children. Unaccompanied children have little control over their immigration process and are typically dependent on an adult to bring them to appointments, interviews, and hearings. They are thus at increased risk of unintentionally missing a scheduled appointment and need flexibility in rescheduling. Instead, under the proposed rule unaccompanied children may suffer severe and permanent consequences—including losing immigration protections—due to circumstances outside of their control. This result thwarts Congress’s intent, through the Trafficking Victims Protection Reauthorization Act (TVPRA),¹⁸⁰ to protect unaccompanied children, recognizing their increased vulnerability and special needs. Nowhere does the TVPRA state or even suggest that unaccompanied children should be susceptible to the loss of protections due to procedural oversights, even when the oversights are properly attributable to the unaccompanied child or the sponsor.

c. DHS Does Not Indicate Clearly How Employers as Petitioners May Be Subject to Biometric Requirements, Causing Concern Regarding Religious Worker Petitions.

The proposed rule makes a point of saying that all immigrants and those associated with requests for immigration benefits, including petitioners, may be subject to biometrics collection. Yet, when discussing the U.S. citizens and permanent residents who may be subject to the requirements, the rule discusses family-based petitions only. It is therefore unclear whether the biometrics requirements will apply to employment-based petitions (other than EB-5 regional centers).

Requiring U.S. Citizen Religious Superiors (signers of the immigrant petitions) to submit to biometrics is invasive and curtails religious freedom in the United States. Religious worker permanent residence cases are “employment” rather than family-based based immigration cases. There is no personal or biological relationship between the employer and the religious worker. To require the employer to submit to biometrics collection is impractical and burdensome. A religious organization may have many leaders who change roles so petitions could have many different signers. Will each signer be required to submit to biometrics? If a signer changes roles in the organization will he/she still be required to submit to biometrics (what happens when leadership changes)? If the signer is unavailable, will the case be delayed? Furthermore, some religious organizations are “cloistered” which means they exist apart from the public world. Living and praying in seclusion is the way of life of these religious orders.

CLINIC, as a stakeholder in the religious visa program, strongly opposes to any requirement on religious employer petitioners to submit biometric data as part of any immigrant petition process because the proposed rule impedes religious freedom by creating a chilling effect where religious organizations will hesitate sponsoring foreign-born religious workers for permanent residence. CLINIC is concerned that many religious leaders will not submit to such a requirement and will

¹⁸⁰ Pub. L. 110-457, 122 Stat. 5044.

instead refrain from sponsoring foreign-born religious workers who are sorely needed to serve their communities of faith.

Moreover, this proposed rule would burden the government and impose extra and unnecessary work on the immigration service. USCIS already has security and verification programs that allow it to fully investigate immigration matters and adjudicate immigration benefits. The R-1 religious worker program already has a mandatory “site visit” requirement where fraud investigators inspect employers and religious workers. These site visits are thorough and exhaustive. Biometric data collection of an employer adds nothing to this already robust regimen. Therefore, this proposed rule provides no significant benefit for government security or verification for immigration processing of religious worker petitions.

IV. DHS SHOULD WITHDRAW ITS PROPOSED CHANGES TO THE GOODMORAL CHARACTER ASSESSMENT FOR VAWA SELF-PETITIONERS AND T-1 STATUS HOLDERS APPLYING FOR ADJUSTMENT OF STATUS

The proposed changes to the good moral character (GMC) 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. Both remedies, for example, have special confidentiality protections, provide for establishing eligibility based on “any credible evidence,” and have specific provisions regarding applicable inadmissibility grounds, eligibility for waivers of inadmissibility, and the assessment of good moral character. The three proposed modifications of GMC assessment, individually and cumulatively, erode the protections accorded to survivors of domestic abuse and trafficking by creating what is certain to be a higher bar for establishing GMC, with greater reliance on subjective determinations by adjudicators.

a. DHS Should Withdraw the Proposed Regulatory Text Expanding the Assessment of GMC to Include Conduct Preceding the GMC Period Established by Current Regulations.

VAWA self-petitioners and T-1 adjustment applicants must establish good moral character for specified periods established by statutory and regulatory provisions. . For VAWA self-petitioners, the specified period is three years preceding the self-petition,¹⁸¹ and for T-1 adjustment of status applicants, GMC must be established from the date of approval of T-1 status through adjudication of the adjustment of status application.¹⁸² The proposed regulation seeks to incorporate a limitless time period for the assessment of GMC for VAWA self-petitioners and T-1 adjustment applications with no corresponding statutory authority to do so, and no credible basis for this regulatory change.

¹⁸¹ *USCIS Memorandum Determinations of Good Moral Character in VAWA-Based Self-Petitions*—HQOPRD 70/8.1/8.2 (Jan. 19, 2005); 61 FED. REG. 13065, 13066 (Mar. 26, 1996).

¹⁸² 8 USC § 245 (1)(1)(B); 8 CFR § 245.23(g)

In justifying this expanded time period for assessing GMC, DHS points to the preamble to the VAWA regulations, also cited in a 2005 USCIS policy memorandum,¹⁸³ which essentially states that the adjudicator can take into account conduct preceding the statutory period. Notably there is no VAWA or T visa statutory authority for creating an expanded time period for examining GMC, nor is there any language in INA § 101(f) to support the consideration of conduct outside the statutory period. Citing the naturalization regulation on GMC,¹⁸⁴ DHS also justifies the change by saying it is consistent with other adjudicative determinations of GMC. Notably, however, Congress expressly authorized the consideration of evidence outside the statutory period for naturalization applicants, with statutory language stating that the adjudication may take into consideration the applicant's conduct at any time prior to filing the application.¹⁸⁵ Under these circumstances, the VAWA regulations preamble and the 2005 USCIS memo are one and the same "authority" and lack any remedy-specific statutory foundation.

In addition, implementation of this proposed change effectively raises the bar for establishing GMC by formalizing the routine consideration of conduct occurring outside the statutory period. As drafted, the starting point for an adjudicator will be the consideration of conduct prior to the specified GMC period, and then determining (a) if the earlier conduct "appears relevant" to assessment of the applicant's GMC, and (b) if the conduct of the applicant during the statutory period does not reflect a "reform of character." This review, which would now become the norm, adds two new subjective determinations to the assessment of GMC without any guidance or criteria about how to evaluate relevancy or character reform.

The inevitable consequence of the proposed text are new opportunities for abuse of discretion, and widely varying case GMC assessments. Under current standards, an applicant for these humanitarian forms of relief can determine eligibility to establish GMC with a fair amount of certainty, with reference to whether she or he has conduct falling within the INA § 101(f) statutory bars or other unlawful conduct during the requisite time period. If the proposed regulatory change is adopted, applicants will have to assume that any prior unlawful acts will routinely be taken into account, regardless of the absence of any GMC bars or other unlawful conduct during the period specified in current regulations.

The proposed text also runs counter to the special exceptions to the GMC statutory bars as applicable to VAWA self-petitioners and T-1 adjustment of status applicants. Under INA § 204(a)(1)(C), and related USCIS policy, where a self-petitioner would otherwise be ineligible to establish GMC based on conduct within the three-year statutory period, the applicant may nevertheless be found to be a person of GMC if the disqualifying conduct was connected to the abuse and is waivable. Similarly, INA § 245(l)(6) provides that T-1 adjustment of status applicants subject to a GMC bar may nevertheless establish GMC if the disqualifying act was caused by or incident to trafficking. While these special policies were enacted in recognition of the special circumstances applicable to survivors of abuse, the proposed regulatory change places more obstacles in the path of establishing GMC.

¹⁸³ *USCIS Memorandum Determinations of Good Moral Character in VAWA-Based Self-Petitions*; Preamble to VAWA regulations, *supra* note 181.

¹⁸⁴ 8 CFR § 316.10.

¹⁸⁵ 8 USC § 316(e)

Finally, it is also worth noting that the proposed text involves a mandated consideration of factors that would otherwise be addressed in the course of related adjudications. For T-1 adjustment applicants, conduct preceding the specified period is already considered with respect to both inadmissibility and discretion. For VAWA self-petitioners, issues of conduct prior to the established GMC period, are likewise considered at the adjustment of status stage, as they relate to both discretion and grounds of inadmissibility. These are the appropriate contexts to address conduct outside the statutory period to the extent that it is relevant to discretion or inadmissibility.

b. DHS Should Withdraw the Proposed Regulatory Text Eliminating the Presumption of GMC For Children Under Age 14.

The presumption of GMC for VAWA self-petitioners and T-1 adjustment applicants under age 14 appropriately recognizes that children cannot reasonably be considered to have the requisite level of independent judgment, maturity and responsibility that may apply to older minors and to adults. In fact, the very nature of the statutory bars listed in INA § 101(f), primarily addressing knowing and intentional conduct, would not be appropriate for a GMC determination given the young age of the juvenile committing the act.

Other provisions and policies in immigration law recognize the need to have different standards for minors because of diminished capacity, including juvenile offenses not being treated as convictions; and the affirmative defense available to persons who made a material misrepresentation for an immigration benefit while under age 18. While USCIS recently removed reference to this affirmative defense in the USCIS policy manual text regarding false claims to citizenship, it was a longstanding explicit policy, and it remains the policy of the Department of State in in the Foreign Affairs Manual in consular processing adjudications.¹⁸⁶ In addition, recent updated policy guidance from USCIS on form I-130 petition adjudication includes enhanced screening of marriages involving a minor, premised, in part, by concerns about the minor's ability to fully and freely consent to the marriage.¹⁸⁷

Although DHS appears to regard this change as insignificant, the presumption of GMC for minors under age 14 communicates an important message to adjudicators regarding the general lack of culpability of children; we appropriately assume they have good moral character because it is not reasonable to hold them accountable, as a matter of character, for any acts that might be violations of law. Without the presumption, we risk seeing officers approach the issue of GMC with minors under age 14 as they would for older minors and adults. Moreover, even with the existing presumption of GMC, the current regulations for self-petitioners and T-1 adjustment applicants allow USCIS to request evidence regarding the GMC of an applicant under age 14 at any time, in its discretion. This should be more than adequate authority for USCIS to seek additional evidence about the GMC of these very young applicants while leaving the appropriate presumption of GMC in place.

¹⁸⁶ 9 FAM 302.9-5

¹⁸⁷ AFM § 21.3(a)(2)(D) as incorporated in USCIS POLICY MANUAL Vol. 6, Part B.

c. VAWA Self-Petitioners Should Not Be Required to Submit Biometrics.

The requirement of making VAWA self-petitioners provide biometrics rather than rely on either police clearance letters or state ID checks may have a chilling effect on applicants who are concerned that potential inadmissibility-related issues may be identified that do not have to do with GMC, but may expose the applicant to enforcement at a stage where there is no concurrent waiver to submit. For example, it is not uncommon for an abused spouse to flee the abuser spouse by going abroad, and then return to the United States based on threats from that same abuser. It is also not uncommon for a person trying to return without documents, including an abused spouse, to be stopped at the border and issued an expedited removal order. At that point, if the abused spouse successfully returns without inspection, she has triggered the permanent bar and is exposed to reinstatement of removal. At the adjustment of status stage, these issues may be addressed with an I-601 waiver and with an I-212 application for advance permission to return. At the I-360 stage, however, it is concerning that the self-petitioner may hesitate to apply knowing that any history of arrest, unrelated to GMC issues, will nevertheless be revealed, and potentially trigger enforcement. Information regarding an applicant's history of crime-related arrests, if any, is already adequately captured by USCIS via the mechanisms identified in the current regulations.¹⁸⁸

V. THE PROPOSED RULE HAS SERIOUS DEFECTS SIMILAR TO THOSE DEFECTS IN A RULE ADDRESSED IN *J.E.C.M. V. LLOYD*

DHS proposes that any applicant, petitioner, sponsor, beneficiary, or individual filing or associated with an immigration benefit or request, including United States citizens, must appear for biometrics collections without regard to age unless DHS waives or exempts the biometrics requirement.

DHS's proposed rule has parallels with a proposed rule put forward two years ago by the Administration for Children and Families, Office of Refugee Resettlement, HHS.¹⁸⁹ ORR's proposed rule would have allowed it to collect biometric data on everyone living in the household of an applicant for sponsorship of an unaccompanied minors in ORR's custody. ORR had already arranged to share this information with ICE and CBP under MOU concluded a few months earlier.

ORR tried twice without success in 2018 to get its rule approved quickly through OMB's "emergency processing procedures." In the end, ORR circumvented the notice and comment process by absorbing the proposed rule into its internal policy guide under the guise it an "interpretative rule." Interpretative rules, in contrast to legislative rules, are described as clarifications of agency readings of existent rules rather than new laws. Different federal agencies have conjured up the respective ways to accomplish the same aim.

¹⁸⁸ 85 FED. REG. at 56338, 56361.

¹⁸⁹ Administration for Children and Families, Submission for OMB Review; Comment Request, 83 FED. REG. 42,895, 42,895 (Aug. 24, 2018).

In *J.E.C.M. v. Lloyd*, a group of plaintiffs sued ORR in a class action in part to defeat ORR's unilateral adopted of the proposed rule as an element of the litigation.¹⁹⁰ ORR moved to have the litigation dismissed. In its Memorandum Opinion, the U.S. District Court for the Eastern District of Virginia granted ORR's motion in part, but it also allowed the plaintiffs to proceed on several counts. Among these were the plaintiffs' challenge to the ORR's handling of the proposed rule regarding sponsors.

J.E.C.M. v. Lloyd is pertinent here because DHS's proposed rule suffers from a serious deficiency that the court detected in ORR's policies. In its Memorandum Opinion, the court agreed with the plaintiffs that ORR had lost its way by becoming more of a law enforcement force than agency aiding immigrant children:

A policy that systematically elevates immigration enforcement over child welfare, one whose effects are to destabilize would-be sponsors' home environments and to discourage potential sponsors from applying for reunification, is flatly inconsistent with ORR's statutory responsibility to care for unaccompanied minors in its custody and release them promptly to safe and stable environments.¹⁹¹

DHS's proposed rule would have similar untoward ramifications. It, too, would deter would-be sponsors and consequently prolong the detention periods of children in ORR custody.

Unlike ORR, DHS comprises several agencies participating in the immigration process some of which are enforcement components. However, while CBP and ICE may be law enforcement arms within DHS's immigration operations, USCIS is not. Instead, USCIS is tasked with determining eligibility for benefits, but are also directed to aid immigrant applicants.

As the proposed rule itself states, DHS engages in the "administration" as well as the enforcement of immigration laws. Among the agency's duties are "the adjudication of benefits."¹⁹² Helping asylum seekers and refugees is one prominent example. Another of those benefits is to work to place unaccompanied children with suitable sponsors. DHS does this task in conjunction with ORR, as directed under the *Flores* Settlement. The agreement requires DHS to unite immigrant children with their parents with alacrity (however much the agency openly chafes at its duty).¹⁹³ The proposed rule acknowledges as much, albeit obliquely, when it mentions sponsors within the domain of persons to be covered by the new biometrics procedures.

The suppression of sponsors is but one predictable outcome of the proposed rule. The new biometric requirement would encompass all immigrants. DHS's attempt to play down this effect by asserting at scattered moments in the rule that the new biometric arrangement is not hostile to

¹⁹⁰ *J.E.C.M. by & Through His Next Friend Saravia v. Lloyd*, 352 F. Supp. 3d 559 (E.D. Va. 2018).

¹⁹¹ *J.E.C.M. v. Lloyd*, et al., 352 F. Supp. 3d at 584.

¹⁹² 85 FED. REG. at 56339.

¹⁹³ *Unaccompanied Alien Children and Family Units Are Flooding the Border Because of Catch and Release Loopholes*, (Feb. 15, 2018), www.dhs.gov/news/2018/02/15/unaccompanied-alien-children-and-family-units-are-flooding-border-because-catch-and#:~:text=The%20Flores%20settlement%20agreement%20has%20now%20been%20litigated,or%20shelter%20situations%20until%20they%20locate%20a%20sponsor.

the interests of immigrants is not facially credible.¹⁹⁴ At other places in the rule, DHS tries different tack. It portrays itself as the restrained custodian of personal data—who is nevertheless compelled to harvest as much personal biological information as it can.¹⁹⁵ In the end, any attempt to dress up the proposed rule as humane and beneficial for immigrants is in vain, as the *J.E.C.M. v. Lloyd* court has already established.

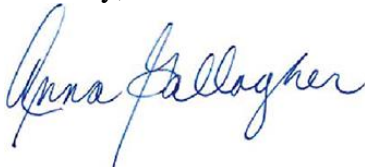
VI. CONCLUSION

This comment, despite its length and detail, are not comprehensive of our objections to the proposed rule. Because we only had 30 days to evaluate the rule and draft this comment, we did not have time to address all of the chilling effects that this rule may have or to evaluate the economic impact of this rule on communities, states, or organizations. Many other facets of this rule exist that we could address if we had sufficient time to analyze and write this comment.

Given the multitude of procedural deficiencies and substantive concerns identified in the promulgation of this rule, we encourage DHS to withdraw this proposed rule. In seeking to accomplish its unsubstantiated goals, this NPRM would drastically increase surveillance of immigrants on an indefinite basis. Indeed, this proposed rule is the precipice of the United States becoming a police state, where privacy and civil liberties become secondary rights, all in the name of fearing rather than welcoming the stranger.

Thank you for the opportunity to submit this comment. We appreciate your consideration. Please do not hesitate to contact Jill Marie Bussey, CLINIC's Advocacy Director, at jbussey@cliniclegal.org should you have any questions about this comment or require further information.

Sincerely,



Anna Marie Gallagher
Executive Director

¹⁹⁴ “The proposed rule would provide benefits that are not possible to quantify. Qualitatively, the proposed rule would provide individuals requesting certain immigration and naturalization benefits with a more reliable system for verifying their identity when submitting a benefit request. This would limit the potential for identity theft while also reducing the likelihood that DHS would be unable to verify an individual's identity and consequently deny the benefit. In addition, the proposal to allow individuals to use DNA testing as evidence to demonstrate the existence of a claimed genetic relationship would provide them the opportunity to demonstrate a genetic relationship using a quicker and more effective technology than the blood testing method currently provided for in the regulations. *See* 8 CFR 204.2(d)(2)(vi).” 85 FED. REG. 56338, 56385.

¹⁹⁵ 85 FED. REG. at 56340, 56351.