October 13, 2020

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

Re: DHS Docket No. USCIS-2019-0007, "Collection and Use of Biometrics by U.S. Citizenship and Immigration Services." 85 Fed. Reg. 56338 (September 11, 2020)

Oxfam America ("Oxfam")[1] and Demand Progress Education Fund (DPEF)[2] submit these comments in response to the Department of Homeland Security's ("DHS") Notice of Proposed Rulemaking regarding the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services. Through its work with immigrant populations in the U.S. and other countries around the world, Oxfam has developed extensive experience and expertise on issues of the protection of immigrant rights, data gathering about immigrants, and regulation of these subjects by various government agencies. DPEF has conducted extensive research into the government's collection and mishandling of information, including invasions of privacy conducted at scale. Oxfam and DPEF appreciate the opportunity to share its perspectives and comment on this proposed rule.

[1] Oxfam is a not-for-profit organization dedicated to ending the injustice of poverty. Oxfam works towards that goal in many different ways, including by working with immigrant populations throughout the United States and analyzing the processing of biometric data by the United Nations High Commissioner for Refugees. Oxfam has published information regarding how that organization processes biometric data (including iris scans) to help determine immigration eligibility of refugees at a given point in time. *Oxfam America, Refugees: Who are they? And other frequently asked questions*, (June 18, 2018), https://www.oxfamamerica.org/explore/stories/refugees-who-are-they-how-does-resettlement-work-and-other-frequently-asked-questions/.

[2] DPEF is a fiscally-sponsored project of New Venture Fund, a 501(c)3 organization. DPEF and our more than two million affiliated activists oppose overly broad surveillance and overly invasive surveillance technologies. A recent example of DPEF's research into unlawful and mishandled surveillance is *Section 215: A Brief History of Violations*, (Sept. 2019), https://s3.amazonaws.com/demandprogress/reports/sec-215-violations-report.pdf.

Information is the new currency, and collecting it is neither simple nor risk free. As DHS formulates regulations for collecting information, particularly information as sensitive as biometric information and from as broad a group of people as the present proposal implicates, DHS should keep a number of considerations top of mind. These considerations include whether the technology for processing the information is sophisticated enough for a government agency to rely on it; whether these shifts are corrosive to individuals' rights with respect to their information; whether the processing of the information is consistent with the data gathering regulations and other standards promulgated by other agencies with experience in similar data gathering efforts; and whether the government agency can effectively protect the information it collects.

Oxfam and DPEF believe DHS's proposed regulations fail to account for these considerations, for reasons that we explain below. We urge DHS to reconsider the proposal in light of the concerns we raise. It is particularly important to move carefully in the area of biometric data collection, an area that is still developing and that raises significant concerns about invasive practices that impinge on individuals' right of privacy. Several agencies, including the Federal Trade Commission ("FTC"), have recognized that biometric data is unique and have promulgated guidance for those who wish to process it. It is important to heed these guardrails to minimize the risk of harm to data subjects.

Unfortunately, the consequences of collecting and using biometric data often surface only after people have been harmed. For example, last month the Office of the Inspector General for the Department of Homeland security ("OIG") released a report noting that traveler images from the U.S. Customs and Border Protection's facial recognition pilot appeared on the dark web. The OIG found that "CBP's information security practices during the pilot were inadequate to prevent the [incident]."[3] Incidents like these create widespread concerns about the potential ramifications of processing biometric data and whether the government should use it. Indeed, the OIG recognized that the recent incident at the CPB "may damage the public's trust in the Government's ability to safeguard biometric data and may result in travelers' reluctance to permit DHS to capture and use their biometrics at U.S. ports of entry."[4]

As discussed further in Section I of these comments, Oxfam and DPEF oppose DHS's proposal to expand its collection and processing of biometric data. DHS's proposal raises particular concerns because the notice does not reflect a process of reasoned decision-making. Instead, it appears that DHS failed to consider the significant costs of its proposal, serious shortcomings of the technology that processes biometric data that may render its proposal ineffective, individuals rights' with respect to their biometric data, and significant concerns expressed by other regulators and legislators regarding the processing of biometric data. [5] DHS

[3] Office of Inspector General, Review of CBP's Major Cybersecurity incident during a 2019 Biometric Pilot, (September 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[4] *Id.*

[5] *Motor Vehicle Manufacturers Association v. State Farm Auto Mutual insurance Co,* 463 U.S. 29, 43 (1983) (explaining that an agency decision is arbitrary and capricious if the agency "entirely failed to consider an important aspect of the problem.").

offers no compelling explanation as to why it should proceed with its proposal in spite of the evidence before the agency that cautions against it. Therefore, as discussed further in section I of these comments, Oxfam and DPEF requests that DHS abandon this proposal in its entirety. If DHS wishes to redraft its proposal, Oxfam and DPEF requests that DHS make the following changes to its current proposed rules to address similar concerns:

- Align the definition of "biometrics" with the definitions used by other agencies with experience in this field;
- Clarify that DHS will use biometric data only for those purposes for which it has given notice;
- Limit the circumstances in which DHS can share biometric data with other agencies;
- Clarify that DHS will collect and process biometric data only when it is efficient (uses technology that is so accurate that government agencies can rely on it) and when there is no alternative source of information; and
- Clarify that DHS will process full DNA profiles only when it has no other alternative.

Section II of these comments considers each of these particular requests in more detail.

I. Oxfam and DPEF Urge DHS To Withdraw Its Proposal To Expand Its Collection and Use of Biometric Data.

A. *DHS's Proposed Use of Biometric Data Ignores Scientific Evidence and Is Inefficient.*

Oxfam and DPEF believes that there are serious flaws with the DHS proposal and that it should be withdrawn in its entirety. While DHS argues that its proposal will increase efficiency and enable DHS to perform its responsibilities more effectively, the record demonstrates that this is not the case. Indeed, the evidence suggests that expanding the use of biometric data as proposed by DHS will both fail to achieve the intended results and increase costs.

DHS alleges that "Biometrics collection upon apprehension or arrest by DHS will accurately identify the individuals encountered, and verify any claimed genetic relationship. This in turn will allow DHS to make better informed decisions as to the processing, transporting, and managing custody of aliens subject to DHS's law enforcement authorities."[6]

However, this assertion ignores several important attributes of biometric data and existing technology, and runs counter to the evidence before the agency. First, using biometric data will not necessarily lead to more accurate identification and verification, as the rule statement suggests. The technology used to process biometric data is still in its infancy,[7] and researchers

[6] 85 Fed. Reg. 56350 (September 11, 2020).

[7] 85 Fed. Reg. 56366 (September 11, 2020) (DHS acknowledged that "The technology for collecting and using biometrics has undergone constant and rapid change.").

are still developing ways to test it effectively.[8] The lack of adequate testing means the technology's accuracy is unclear. This creates serious uncertainty about the efficacy or efficiency of processing biometric data for identification and verification purposes. Therefore, it is highly implausible that DHS's collection of biometrics will lead to more accurate verification and identification.[9]

The National Institute of Standards and Technology ("NIST"), a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce, has identified several problems in using biometric data and related technology for identification and verification. Just last year, that organization evaluated the effects of race, age, and sex on face recognition software. NIST found that the accuracy of face recognition software tools depends on the algorithm, and "the majority of face recognition algorithms exhibit demographic differentials… [i.e., the] algorithm's ability to match two images of the same person varies from one demographic group to another."[10] This study, in particular, highlights the potential issues in using face recognition technology across populations as diverse as immigrants and those seeking immigration benefits. Because the algorithms are not consistently effective, DHS would have to accept that its use of facial recognition technology will lead to inaccurate results.

Irises present similar variability issues. While irises were once lauded as a strong biometric, studies have demonstrated that as individuals age, it becomes increasingly difficult to recognize their irises. One study found that a period as short as three years can make iris recognition more difficult, and a different NIST study found that over a period of ten years there will be consistent change in the distinctive textures of individual irises.[11] Voiceprints are prone to similar inconsistencies. At the RSA conference in 2017, Dr. Eli Khoury presented a study that demonstrated a degradation in performance of modern speaker recognition systems over just four

---

[8] National Institute of Standards and Technology ("NIST"), NIST Releases Data to Help Measure Accuracy of Biometric Identification (December 2019), https://www.nist.gov/news-events/news/2019/12/nist-releases-data-help-measure-accuracy-biometric-identification (announcing that NIST released its first ever multimodal data set (i.e., a data set that links an individuals' biometric markers together for use by systems that want to use multiple biometric markers for identification)).

[9] *Motor Vehicle Manufacturers Association,* 463 U.S. 43 (explaining that an agency decision is arbitrary and capricious if the agency's decision "is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.").

[10] NIST, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, (December 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[11] NIST, NIST Study Advances Use of Iris Images as a Long-Term Form of Identification, (August 20, 2019), https://www.nist.gov/news-events/news/2013/08/nist-study-advances-use-iris-images-long-term-form-identification ("A new report by biometric researchers at [NIST] uses data from thousands of frequent travelers enrolled in an iris recognition program to determine that no consistent change occurs in the distinguishing texture of their irises for at least a decade… A study of 217 subjects over a three-year period found that the recognition of the subjects' irises became increasingly difficult, consistent with an aging effect.").

months.[12] This study underscored that voices change over time. Thus, scientific evidence raises significant doubt that DHS will be able to rely on biometric data it collected from an individual to accurately identify that individual years later. Given the rate at which children grow and change, it is even more doubtful that DHS will be able to rely on biometrics collected from a minor to reliably identify that individual as an adult.

Using fingerprints and palm prints for verification and identification purposes also presents risks. Specifically, such prints can be left behind in public places, leaving them vulnerable to bad actors who can lift them and use them for nefarious purposes. There is a similar vulnerability in voice prints, iris prints, and face prints. Because individuals cannot function in society without generating and being associated with their biometric data, bad actors have unique opportunities to capture and manipulate that data. The ease with which biometric data can be manipulated renders it particularly ill-suited for identification and verification. Unlike in the case of an alien number or a green card, an individual cannot apply for a replacement if a bad actor steals his or her biometric data. Thus, it is of critical importance that any entity (even a government agency) collects biometric data only when there is no other alternative, if ever.

Moreover, biometric data is very expensive to collect and protect. Government agencies that wish to collect biometric data must expend significant resources protecting that data. As discussed above, biometric data is extremely likely to trigger technical challenges and is extremely susceptible to fraudulent use. Consequently, agencies that wish to rely on it for identification purposes will have to spend significant resources to make sure they accurately process and fulsomely protect it. Therefore, agencies that wish to collect, process, and store biometric data will need to structure their cybersecurity systems to protect it. The World Bank recognized this when it stated, "the collection and use of biometric data presents some particular data protection and exclusion risks and can significantly add to the cost of the ID system and add operational complexity."[13]

In issuing its proposal, DHS appears not to have taken full account of these numerous concerns with increasing the use of biometric data. DHS should withdraw the entire proposal and reexamine it in light of the concerns raised by the record.

B. *DHS's Proposed Rule Lacks any Analysis of Impacts on Current Backlogs within DHS.*

Collection of the proposed additional biometric data under the proposed rule not only poses significant inefficiency concerns, but will exacerbate existing backlog issues within DHS and USCIS in a way not adequately considered or analyzed by the proposed rule statement of costs and benefits. DHS estimates that the proposed rule would increase the total number of

[12] RSA Conference, The Problem of Voice Aging in Biometric Security, (February, 17, 2017), https://www.rsaconference.com/usa/us-2017/agenda/the-problem-of-voice-aging-in-biometric-security.

[13] The World Bank, Biometric data, https://id4d.worldbank.org/guide/biometric-data.

annual biometrics screenings from 3.9 million to 6.07 million, a roughly 50% increase.[14] Under existing rules, there is a biometrics collection rate of 46% across all forms, which would increase to a 71% collection rate under the proposed rule.[15] Nowhere in the proposed rule and accompanying statement does DHS analyze the ways in which increased collection, processing, and storing of the expanded biometrics data will impose burdens on both the agency and applicants for immigration benefits, but instead relies on a cursory statement that the proposed rule will uniformly decrease administrative burden.[16]

Dramatically expanding the types and amount of data collected will undoubtedly increase the USCIS's ever-increasing backlog of applications. Despite a 10% drop in applications received by USCIS between the end of fiscal year 2017 and fiscal year 2019, the overall case processing time over that same period rose by 25%: from eight months to ten months.[17] These processing delays layer on top of a ballooning backlog of cases. At the close of calendar 2019, USCIS had 5.5 million applications pending, up nearly 2.2 million from the close of calendar 2015.[18] This backlog existed under the current rules, which only require biometrics for those applications which require a background check.

This backlog has only been further exacerbated by the coronavirus pandemic. USCIS closed its offices in March, which required Applications Support Centers to cancel and reschedule biometrics appointments, delaying applications by months. Indeed, some of these centers are just now offering biometric screening appointments for the first time in October.[19] While USCIS avoided a furlough of nearly 70% of its workforce in August, USCIS itself acknowledged that the costs associated with avoiding the furlough came at "a severe operational cost that will increase backlogs and wait times across the board."[20]

The backlog of applications and existing processing delays have measurable negative consequences for U.S. businesses, families, and the individuals seeking immigration benefits.

---

[14] 85 Fed. Reg. 56378 (September 11, 2020).

[15] 85 Fed. Reg. 56343 (September 11, 2020).

[16] 85 Fed. Reg. 56369 (The only stated rationale for the proposed program is that it is "conducive and relevant to the evolution to a person-centric model for organizing and managing of immigration records.").

[17] AILA Policy Brief: Crisis Level USCIS Processing Delays and Inefficiencies Continue to Grow. (February 26, 2020) https://www.aila.org/advo-media/aila-policy-briefs/crisis-level-uscis-processing-delays-grow.

[18] Center for Immigration Studies, "USCIS Has 5.5 Million Applications Pending, Up 2.2 Million from 2015," (June 26, 2020) https://cis.org/North/USCIS-Has-55-Million-Applications-Pending-22-Million-2015.

[19] Genevieve Douglas, "Biometric Appointment Delays Threaten Visa Work Permits," Bloomberg News (August 12, 2020) https://news.bloomberglaw.com/daily-labor-report/biometric-appointment-delays-threaten-visa-work-permits.

[20] USCIS, "USCIS Averts Furlough of Nearly 70% of Workforce." (August 25, 2020) https://www.uscis.gov/news/news-releases/uscis-averts-furlough-of-nearly-70-of-workforce.

The proposed rule statement fails to analyze or consider the proposed rule's likely effects of delaying processing times and increasing the existing application backlog. Indeed, these likely consequences would directly undercut the stated purpose of the rule to improve the "efficiency in identity verification."[21]

The proposed rule should be accompanied by an in-depth analysis of the true costs of its implementation against the measurable benefits and effects so that stakeholders can accurately assess its value.

C. *DHS's Proposal Does Not Give Appropriate Weight to the Rights of the Data Subjects.*

The United States Constitution creates a privacy interest in avoiding the disclosure of personal matters. The U.S. Supreme Court has recognized this interest on multiple occasions.[22] Given that individuals cannot function without society associating them with their biometric data, it is hard to conceptualize a form of information that is more personal than biometric data. Therefore, the Constitution protects individuals' interest in avoiding the disclosure of personal information such as biometric information.[23]

Furthermore, the United Nations has recognized a human right to privacy. Specifically, Article 12 of the United Nations Declaration of Human Rights reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[24] Similarly, in 1992, the U.S. signed and ratified the International Convention on Civil and Political Rights, which recognizes, "No one shall be subjected to arbitrary or unlawful interference with his privacy... Everyone has the right to the protection of the law against such interference or attacks."[25] Thus, even if an individual does not enjoy particular protections of the U.S. Constitution, that individual still has a right to their privacy.

---

[21] 85 Fed. Reg. 56344 (September 11, 2020).

[22] *Whalen v. Roe*, 429 U.S. 589, 599–600, 97 S.Ct. 869, 51 L.Ed.2d 64; *Nixon v. Administrator of General Services*, 433 U.S. 425, 457, 97 S.Ct. 2777, 53 L.Ed.2d 867.

[23] *Cf. Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (analyzing the development of constitutionally protected zones of privacy and the Supreme Court's views regarding developing technology's intrusions on the right to privacy and concluding "that an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'").

[24] United Nations, Universal Declaration of Human Rights, (December 10, 1948), https://www.un.org/en/universal-declaration-human-rights/#:~:text=No%20one%20shall%20be%20subjected%20to%20arbitrary%20interference%20with%20his,against%20such%20interference%20or%20attacks.

[25] United Nations Human Rights, Office of the High Commissioner, (March 23, 1976) https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

That right applies to protect the individual's biometric information from arbitrary interference, and the U.S. must honor it.

The U.S. Constitution, the Universal Declaration of Human Rights, and the International Convention on Civil and Political Rights all protect individuals' ability to control their information. By collecting biometric information and processing it in perpetuity and for vaguely defined reasons, DHS's proposal diminishes that control.[26]

DHS's proposal contains a mere conclusory statement that "This rule would not cause the taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights."[27] There is no explanation of how the collection of this intensely personal information from U.S. citizens will be managed to protect their constitutional interest in informational privacy. Moreover, there is no consideration of how this rule impinges on the privacy rights of non-U.S. Citizens as recognized by the United Nations. Even if DHS has reasoned justifications for impinging on individuals' right to privacy, the complete lack of substantive analysis warrants reconsideration, if not withdrawal, of this proposal.

D. *DHS's Proposal Fails To Give Proper Attention to Guidance Issued by Authorities With Deep Experience Regulating Data.*

DHS should also reconsider its proposal in light of the guidance provided by government authorities with longer and deeper experience with regulation of the collection and handling of data, including biometric data. Indeed, DHS's proposal completely disregards the Federal Trade Commission's guidance strongly urging the adoption of data minimization principles.[28] These principles obligate entities to use the least sensitive data for a given purpose. DHS's proposal disregards this guidance. DHS acknowledges that it has existing mechanisms for identifying immigrants, criminals, and applicants for immigration benefits, as well as associated parties.[29] These mechanisms rely on less sensitive data that can be gathered through less invasive

[26] *See, e.g.*, Proposed Rule 8 C.F.R. § 103.16(a)(2) ("DHS may collect biometrics for an individual more than once or, at its discretion, reuse previously collected biometrics, as necessary.").

[27] 85 Fed. Reg. 56413 (September 11, 2020).

[28] *See, e.g.*, Federal Trade Commission, Start with Security: A Guide for Business (June 2015), ("Don't collect personal information you don't need."); Federal Trade Commission, Internet of Things, Privacy & Security in a Connected World, ("Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it… Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event.").

[29] *See, e.g.*, 85 Fed. Reg. 56351 (September 11, 2020) (explaining that DHS relies on declared biographic data for managing identity in the immigration life cycle); *Id.* at 56353 (explaining that DHS collects documentary evidence to verify identity and familial relationships and preclude imposters; these types of documentary evidence include marriage and birth certificates, medical records, school records, religious documents, and affidavits).

processes (e.g., sworn statements). Instead of meeting the FTC's data minimization principles, grounded in that agency's far deeper wealth of experience regulating data, DHS proposes an ill-advised path in which it will collect more sensitive data that is both unnecessary and unlikely to better serve DHS's purposes.

DHS's proposal also ignores state regulatory agencies' recognition that biometric data is a unique form of personal data that warrants unique treatment. Multiple states have conditioned companies' collection of biometric data on appropriate notice and consent procedures, limited sharing of the data, and limited retention of it.[30] By contrast, DHS has already collected biometric data without appropriate notice,[31] and proposes to share it freely amongst law enforcement agencies and to store it in perpetuity.[32] DHS's processing of biometric data raises many of the same concerns as private companies' processing of biometric data. When DHS processes biometric data, individuals still have rights to control their information, and their information is still attractive to hackers. However, because the consequences of DHS's misuse of biometric data are so significant, DHS should hold itself to a higher standard. DHS needs to enhance its efforts to make sure individuals understand what data it collects and how that data will be processed. Moreover, DHS should reevaluate the broad disclosures and retention periods of biometric data contemplated by its proposal.

State legislatures and cities around the country have recognized that governments should not have broad access to biometric data. Several cities including Boston, San Francisco, and Portland have adopted bans limiting government applications of face recognition technology.[33]

---

[30] Wash. Rev. Code Ann. § 19.375.020(1) (requiring notice and consent before enrolling biometric identifiers); Tex. Bus. & Com. Code Ann. § 503.001(b) (requiring notice and consent before capturing biometric identifiers); 740 Ill. Comp. Stat. Ann. 14/15(b) (requiring notice and consent before collecting biometric identifiers); Wash. Rev. Code Ann. § 19.375.020(3) (requiring consent before disclosing biometric identifiers); Tex. Bus. & Com. Code Ann. § 503.001(c)(1) (limiting the ability to disclose biometric data); 740 Ill. Comp. Stat. Ann. 14/15(b) (placing conditions on disclosures of biometric data); Wash. Rev. Code Ann. § 19.375.020((4)(b) (prohibiting retention of a biometric identifier for longer than reasonably necessary to satisfy certain purposes); Tex. Bus. & Com. Code Ann. § 503.001(c)(3) (requiring destruction of biometric data no later than one year after fulfilling the purpose for which it was collected), 740 Ill. Comp. Stat. Ann. 14/15(a) (requiring destruction of a biometric identifier no later than three years after the individual's last interaction with the private entity).

[31] United States Government Accountability Office, FACIAL RECOGNITION CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, (September 2020), https://www.gao.gov/assets/710/709107.pdf (finding that the U.S. Customs and Border Patrol Agency had "not consistently provided complete information in privacy notices or ensured that notices were posted and visible to travelers.").

[32] *See, e.g.*, 85 Fed. Reg. 56352 (September 11, 2020) ("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… it may share DNA test results, which include a partial DNA profile, with other agencies…").

[33] City of Boston Code § 16-62; City of San Francisco Administrative Code, Chapter 19B; City of Portland Ordinance Code, Title 34, Ordinance No. __, "Prohibit the use of Face Recognition (continued…)

These legislative developments underscore that DHS should exercise caution in expanding its processing of biometric data and disclosing it to other agencies.

E. *DHS Needs To Improve Its Cybersecurity Practices Before Collecting Additional Sensitive Data.*

DHS should consider that its current information security program may not be capable of protecting the biometric data it proposes to collect. The OIG's recent evaluation of DHS's Information Security Program for Fiscal Year 2019 found that DHS did not have an effective strategy or department-wide approach to manage risks for all of its systems, did not have a comprehensive strategy or organization-wide continuous monitoring approach to address all requirements and activities at each organizational tier, and apparently had not made progress since prior years.[34]

Each of these concerns have serious implications for DHS's proposed collection of biometrics. Because DHS's proposal envisions such a broad use of biometric data, it is conceivable that several branches of the department will process and have access to the biometric data. If DHS continues to lack central management of cybersecurity risk, it is entirely possible that when one branch's repository of biometric data falls victim to a cyberattack, the other branches will not be aware of the attack and will not appropriately secure their own systems before falling victim to the same attack. Without a comprehensive strategy to monitor the tiers of DHS's cybersecurity program, one system may fall behind the rest of the organization's efforts to protect data. Hackers may be able to access that one system to access DHS's biometric data, even if that system doesn't store it.[35]

Before processing any additional data, DHS should address the concerns raised in the OIG's evaluation of DHS's Information Security Program for Fiscal Year 2019. Given the sensitivity of biometric data, DHS should go beyond the recommendations in the report and confirm that it uses best-in-class technology to protect the biometrics it proposes to collect. The absence of this confirmation could lead to significant consequences. For example, if hackers breach a system and steal biometric data, the data subjects would forever lose control over a crucial part of their identity. In light of the drawbacks of attempting to use biometric data for identification and verification purposes, the legal guidance from agencies with extensive experience with data regulation cautioning against broader uses of biometric data, and the OIG's findings related to DHS's cybersecurity practices, DHS should not expand its processing of

---

Technologies by Private Entities in Places of Public Accommodation in the City," adopted Sept. 9, 2020.

[34] Office of Inspector General, Evaluation of DHS' Information Security Program for Fiscal Year 2019 (REDACTED), (September 30, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-20-77-Sep20.pdf.

[35] Hackers have been able to use vulnerabilities in one system to access another. F.T.C., Start with Security: A Guide for Business, (June 2015), ("The FTC alleged that the company didn't sufficiently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks.").

biometric data. Oxfam and DPEF respectfully request that DHS withdraw its proposed rule and instead, at a minimum, align its practices with the FTC's data minimization principles and the urgent cybersecurity recommendations highlighted in the OIG's evaluation. This path forward avoids unnecessarily expending resources to collect data that will not meaningfully further DHS's identification and verification goals and that could be vulnerable to cyberattacks.

F. *DHS's Proposed Continuous Vetting Program Creates a Significant Burden on the Agency, Applicants, and Employers.*

DHS's proposed rule to create a continuous immigration vetting program lacks any explanation for or evidence of a demonstrated need. Under current rules, individuals with certain types of criminal convictions or those who pose a threat to national security or public safety are not eligible for certain benefits.[36] DHS's only stated rationale for the proposed program is that it is "conducive and relevant to the evolution to a person-centric model for organizing and managing of immigration records."[37] DHS has not provided any reasoning as to why the expansion of continuous vetting and evaluation to legally present applicants for immigration benefit is necessary to the agency's execution of its statutory obligations or why existing monitoring practices requiring the submission of criminal records are insufficient.

Further, the proposed rule creates burdensome and invasive procedures. The proposed rule may require employers serving as authorized signatories or otherwise associated with a petition themselves to submit to biometrics screenings, even if they are U.S. citizens. The rule statement does not address why the extension of screenings to U.S. citizens may be necessary or beneficial to the existing reliability of immigration benefit applications, let alone within the context of an entirely new vetting program.

The proposed rule also does not make clear how sponsoring organizations for employment-based permanent residence filings or for adjustment of status to permanent residence could be subject to the expanded biometrics collection. These businesses and sponsoring organizations have already been negatively impacted by delays in visa processing times, and the proposed rule and its dramatically expanded continuous vetting program will only exacerbate that ongoing harm.

II. In the Alternative, DHS Should Revise the Proposed Rule in Light of the Evidence Before the Agency.

In the event DHS insists on pushing this proposal forward despite the record evidence that counsels against it, Oxfam and DPEF respectfully requests that the agency makes make the changes discussed below. Our proposed changes reflect an analysis of the sections that (1) most significantly depart from existing standards promulgated by regulators, (2) are in tension with recent legislative developments, and (3) are likely to result in inaccurate results from processing biometric data.

[36] 85 Fed. Reg. 56353.

[37] 85 Fed. Reg. 56369.

A. *The Definition of "Biometrics" Should Align With State Definitions of That Term.*

As a preliminary matter, Oxfam and DPEF endorses DHS's decision to exclude from the definition of "biometrics" in the text of the rule certain problematic concepts that appear in the Summary of Proposed Changes. The definition of "biometrics" that appears in the summary of proposed changes includes a vague incorporation of future technologies.[38] It is unclear from that language what these technologies are, what standards they must meet, or even how they will be used. DHS presumably recognized that (1) incorporating the vague reference to future technology would fail to give appropriate notice to the public of the proposal and its substance[39] and (2) could result in reliance on untested and unreliable technology. Instead, if DHS were to insist on adopting this rule, it should rely only on that technology that have proven to be the most reliable.

Oxfam and DPEF also endorse DHS's conclusion that the proposed rule's definition of biometrics should not include "photographs of physical or anatomical features such as scars, skin marks, and tattoos."[40] Such photographic evidence should not be classified as "biometric data." It is not clear whether any of these features are permanent. Additionally, bad actors could get the exact same tattoos, scar their skin in the same way, or mark their skin to match a photograph. Furthermore, the quality of a photograph may detract from the accuracy of identifying a tattoo.[41] Indeed, the quality of an image of any biometric data can introduce errors into identification processes that rely on that photograph to assess biometric data.[42]

---

[38] 85 Fed. Reg. 56355 ("DHS proposes to begin requesting biometric collection (now and through merging technologies) with the following additional biometric modalities: Iris, palm, face, voice, and DNA.").

[39] *See, e.g.,* 5 U.S.C. § 533(b) (requiring agencies to provide the public with adequate notice of a proposed rule followed by a meaningful opportunity to comment on the rule's content; *Connally v. General Construction Co.*, 269 U.S. 385, 391 (1926) ("a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates the first essential of due process of law.").

[40] *Id.*

[41] NIST, Nothing Says You Like a Tattoo: NIST Workshop Considers Ways to Improve Tattoo Recognition, (June 8, 2015), https://www.nist.gov/news-events/news/2015/06/nothing-says-you-tattoo-nist-workshop-considers-ways-improve-tattoo (in which a computer scientist acknowledged that "improving the quality of tattoo images during collection is another area that may also improve recognition accuracy").

[42] *See, e.g.*, NIST, NIST: Performance of Facial Recognition Software Continues to improve, (June 3, 2014), https://www.nist.gov/news-events/news/2014/06/nist-performance-facial-recognition-software-continues-improve ("No algorithms worked well with the webcam images."). El-Abed, M., Charrier, C. & Rosenberger, C. Quality assessment of image-based biometric information. *J Image Video Proc.* **2015,** 3 (2015). https://doi.org/10.1186/s13640-015-0055-8 ("The quality of biometric raw data is one of the main factors affecting the overall performance of biometric systems. Poor biometric samples increase the enrollment failure and decrease the system performance.").

However, the definition of "biometrics" in the proposed rule is still far too broad. In particular, the definition includes "partial DNA profiles." The proposed rule does not explain what "partial" means. Given the significant consequences of DHS processing biometric data (including potentially denying benefits to immigrants who are entitled to them and granting benefits to individuals who are not), DHS should not accept results that are based on a portion of DNA data points. Additionally, it is not clear what "partial" signifies, but it is worth noting that DNA tests (like many other tests) are subject to false positives and false negatives. The inclusion of "partial tests" in the definition of "biometrics" dilutes the value of the evidence DHS proposes to collect since parts of DNA profiles may be even more vulnerable to flaws than tests of the entire profile.[43]

More broadly, DHS's proposed definition of biometric data departs from the definitions that various state governments have endorsed and relied upon. Oxfam and DPEF suggest that DHS edit the proposed definition of biometrics to (1) clarify that biometric data does not capture the problematic types of data referenced in the summary of proposed changes, (2) avoid incorporating unspecified new forms of biometric data that are likely to introduce inaccuracies into the verification and identification process, and (3) bring its definition of biometric data into alignment with that of other agencies, including state agencies that regulate data collection and processing. To that end, we recommend the following red edits to the existing proposed 8 C.F.R. § 1.2:

> "Biometrics" means the measurable biological (anatomical and physiological) ~~or behavioral~~ characteristics of an individual, ~~including~~ an individual's fingerprints, ~~palm prints,~~ ~~photograph (facial image),~~ ~~signature,~~ **retina or** iris **scan** ~~(iris image),~~ ~~voice~~ ~~(~~voice print, **or scan of hand or face geometry**~~), and/or DNA (partial DNA profile)~~ **that is used to identify a specific individual** (subject to the limitations in 8 C.F.R. 103.16(d)(2))."

B. *The Rules Should Minimize the Collection of Biometric Data*.

Given the sensitivity of biometric data (as recognized by the FTC, the World Bank, and various states and cities), agencies should carefully draft their regulations to minimize processing of biometric data. Agencies should collect biometric data from only those individuals whose biometrics lend themselves to identification and only when processing biometric data is the only way to achieve its goals.

DHS currently proposes to collect biometric data from anyone "associated with" a request for a benefit or a form of relief. DHS does not define what constitutes an association with a request, which could lead to the collection of biometric data from an absurdly large group of people. The officer processing the request could be said to have an association with the request. Presumably, DHS has vetted its own employees and does not need to waste taxpayers' money

[43] JSTOR Daily, How Forensic DNA Evidence Can Lead to Wrongful Convictions, (December 6, 2017), ("Partial profiles will match up with many more people than a full profile. And even full profiles may match with a person other than the culprit.").

collecting and protecting biometric data of these employees or acting on waivers of collection of biometric data from them.

Additionally, there is no need to collect biometric data from all individuals applying for an immigration benefit or immigration relief. DHS recognized this when it preserved the ability to waive requests for biometric data from individuals applying for immigration relief and benefits. Furthermore, some of these individuals will be members of populations for whom the technology for processing biometric data tends to be less effective. As discussed above, facial recognition technology does not work equally well across genders and races. The agency should not eschew identification methods that are more reliable for these individuals in favor of technology that will be ineffective to identify them, and should be expected to have disproportionate, negative effects on historically targeted populations.

Collecting biometrics from children for purposes of identification appears to be especially ineffective. As children age, their irises and voices change. Therefore, their biometric data is more likely to lead to inaccurate identifications in the future. Notably, collecting biometric data from children is in tension with recognition from federal lawmakers, federal agencies, and the State of California that children's privacy deserves protection.[44] Moreover, collecting biometric data from children raises unique concerns in light of their lack of agency. If an adult objects to DHS's collection of the adult's biometric data, the adult can withdraw from the immigration process. However, if a child objects to DHS's collection of the child's biometric data, the child may have no recourse. The child cannot return to their country of origin if their guardian wishes to stay in the United States. Therefore, DHS should not pursue collecting biometric data from children.

To appropriately minimize the collection biometric data (that will be expensive to maintain and protect), we proposes the following red edits:

> 8 C.F.R. § 103.16(a)(1): Any applicant, petitioner, sponsor, derivative, dependent, beneficiary, or individual filing ~~or associated with~~ benefit requests as defined in this chapter, or any other request or form of relief, must submit biometrics to DHS in the event there is no other information the agency can use to verify the individual. ~~unless the request is exempted or the requirement is waived by DHS. DHS may waive the requirement in accordance with paragraph (a)(5) of this section, a Federal Register notice, or as otherwise provided by law or regulation.~~ This section applies only to individuals

[44] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. § 6501, *etc*. (protecting children's data from excessive processing and retention); Cal. Civ. Code §1798.120(d) (permitting minors to opt into sales of their data); Ed Markey, Senators Markey and Hawley Introduce Bipartisan Legislation to Update Children's Online Privacy Rules, (March 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-hawley-introduce-bipartisan-legislation-to-update-childrens-online-privacy-rules, (quoting Senator Hawley saying "Big tech companies know too much about our kids, and even as parents, we know too little about what they are doing with our kids' personal data. It's time to hold them accountable…Congress needs to get serious about keeping our children's information safe, and it *begins* with safeguarding their digital footprint online.") (emphasis added).

submitting applications, petitions, or requests to USCIS, including United States citizens~~, without regard to age~~.

***New Sections* 8 C.F.R. §§ 103.16(e), 210.2(c), 210.5(c), 245a.2(d)(3), 264.1(h): Nothing in this section permits DHS to request or require the submission of biometrics if there is another source of information that can be used to identify the individual.**

8 C.F.R. § 245a.2(d): Evidence to support an alien's eligibility for the Legalization Program must include documents establishing proof of identity, proof of residence, and proof of financial responsibility, as well as ~~biometrics and~~ a completed medical report of examination. Such evidence may include biometrics, consistent with 8 C.F.R. § 245a.2(d)(3). All documentation submitted will be subject to verification. USCIS may deny applications submitted with unverifiable documentation. Failure by an applicant to authorize release to USCIS of information protected by the Privacy Act and/or related laws in order for USCIS to adjudicate a claim may result in denial of the benefit sought. Acceptable supporting documents for these three categories are discussed below.

8 C.F.R. § 245a.2(d)(2)(ii): The most persuasive evidence is a document issued in the assumed name which identifies the applicant ~~by biometrics~~. Other evidence which will be considered are affidavit(s) by a person or persons other than the applicant, made under oath, which identify the affiant by name and address, state the affiant's relationship to the applicant and the basis of the affiant's knowledge of the applicant's use of the assumed name. Affidavits accompanied by a photograph which has been identified by the affiant as the individual known to affiant under the assumed name in question will carry greater weight.

8 C.F.R. § 264.1(g): Within 30 days after reaching the age of 14, any alien in the United States not exempt from alien registration under the INA and this chapter must apply for registration and submit biometrics, unless biometrics collection is waived by USCIS or not required consistent with 8 C.F.R. § 264(h). ~~This requirement does not preclude DHS from requiring any alien under the age of 14 who is not exempt from alien registration to submit biometrics.~~

(1) *Permanent residents*. If an alien who is a lawful permanent resident of the United States is temporarily absent from the United States when he or she reaches age 14, he or she must apply for registration and submit biometrics within 30 days of his or her return to the United States in accordance with applicable form instructions; provided that the alien will not be obligated to submit biometrics if USCIS has another way of identifying the alien. Furthermore the alien must surrender any prior evidence of alien registration and USCIS will issue the alien new evidence of alien registration.

C. *DHS Should Limit Use of Biometric Data to Those Purposes for Which it Gave Notice.*

Every state that passed a law that specifically regulates biometric data has recognized that individuals should understand how their biometric data will be used.[45] The FTC has further encouraged companies to give notice and obtain consent when they wish to process data for a materially different purpose.[46] Given the sensitivity of biometric data and the challenges DHS will faces in processing biometric data (e.g., maintaining transparency and protecting, storing, and maintaining biometric data), DHS should likewise commit to notifying individuals of uses of their data and any new uses of data that DHS previously collected. Accordingly, Oxfam and DPEF proposes the following edits in red to:

> 8 C.F.R. § 103.16(a)(2): *Frequency of submission*. DHS may collect biometrics for an individual more than once ~~or, at its discretion, reuse previously collected biometrics,~~ as ~~necessary~~ **contemplated by this title.**
> 8 C.F.R. § 103.16(d)(1) *Biometrics other than DNA*. DHS may store biometrics, other than raw DNA, submitted by an individual as required by this section and use ~~or reuse~~ these biometrics to conduct background and security checks, verify identity, produce documents, determine eligibility for immigration and naturalization benefits, or as necessary for administering and enforcing immigration and naturalization laws.

D. *DHS Should Have a Limited Ability To Share Biometric Data with Other Agencies.*

Every state that has passed a law that regulates biometric data specifically prohibits the free sharing of biometric data.[47] California declines to permit broad sharing of biometric data with government agencies.[48] Given the significant concerns around sharing this data with governmental agencies reflected in decisions by state legislatures and codified in city

[45] Wash. Rev. Code Ann. § 19.375.020(1) (requiring notice and consent before enrolling biometric identifiers); Tex. Bus. & Com. Code Ann. § 503.001(b) (requiring notice and consent before capturing biometric identifiers); 740 Ill. Comp. Stat. Ann. 14/15(b) (requiring notice and consent before collecting biometric identifiers).

[46] *See, e.g.*, Protecting Consumer Privacy in an Era of Rapid Change, 58.

[47] ; Wash. Rev. Code Ann. § 19.375.020(3) (requiring consent before disclosing biometric identifiers); Tex. Bus. & Com. Code Ann. § 503.001(c)(1) (limiting the ability to disclose biometric data); 740 Ill. Comp. Stat. Ann. 14/15(b) (placing conditions on disclosures of biometric data).

[48] California Assembly Bill 1416, 2019.

ordinances,[49] Oxfam and DPEF propose the following red edits to the language from 8 C.F.R. § 103.16(d)(1):

> Biometrics collected, other than DNA, may be shared with appropriate federal, state, and local law enforcement; or intelligence community entities; foreign governments, as authorized by law and/or international agreements, but only **as needed to prevent imminent death or significant bodily injury**.

E. *The Rules Should Clarify That DHS Will Process Full DNA Profiles and Only When There is No Alternative Source of Information.*

DHS should impose additional limitations on the use of DNA data because of the special sensitivity of such data. The mere availability of DNA testing is not sufficient to justify its use. DNA testing is invasive, and DNA is immutable. If the results of a DNA test fall into the wrong hands, the data subject has no recourse to protect his or her genetic makeup and has no hope of the data losing its utility with respect to the bad actor who acquired it. The extremely dangerous consequences if bad actors were to acquire DNA data necessitate requiring a strong and particularized justification for collecting it. DHS has not provided such a justification. Moreover, as the Office of Inspector General's evaluation of DHS's information security program indicates, DHS may not be able to protect DNA data. Finally, as scholars have noted, relying on partial DNA profiles may lead to inaccurate conclusions. Accordingly, Oxfam and DPEF propose the following edits to 8 C.F.R. § 103.16(d)(2):

> (i) DHS may require, request, or accept the submission of DNA or DNA test results to verify a claimed genetic relationship or determine whether a genetic relationship exists if there is no other way to perform the verification or make the determination. DHS may use and store DNA test results~~, which include a partial DNA profile,~~ as evidence of a claimed genetic relationship~~:~~
>
> ~~(A) T t~~o determine eligibility for immigration and naturalization benefits; ~~or,~~
>
> ~~(B) To perform any other functions necessary for administering and enforcing immigration and naturalization laws.~~
>
> ~~(ii) DHS may at its discretion consider DNA test results, which include a partial DNA profile, as primary or secondary evidence of the claimed genetic relationships for any benefit or request.~~
>
> (iii) DHS will only use and handle raw DNA as long as necessary to obtain DNA test results~~, which include a partial DNA profile~~. DHS will destroy raw DNA once these test results are obtained, and DHS will not share DNA test results unless required by law. The DNA test results~~, which include a partial DNA profile,~~ on any individual obtained as part of the benefit request will remain a part

[49] California did not pass Assembly Bill 1416 in 2019. *See*, City of Boston Code § 16-62; City of San Francisco Administrative Code, Chapter 19B; City of Portland Ordinance Code, Title 34, Ordinance No. __, "Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City," adopted Sept. 9, 2020.

of the file and record of proceeding, DHS will store and may share DNA test results, which include a partial DNA profile, for immigration adjudication purposes or for law enforcement purposes to the extent permitted by law and as needed to prevent imminent death or significant bodily injury.

Oxfam and DPEF appreciate DHS's consideration of these comments. We look forward to continuing to work with DHS on these critically important issues.

Sincerely,

Noah Gottschalk
Humanitarian Policy Lead
Oxfam

Vicki Gass
Senior Policy Advisor
Oxfam

Sean Vitka
Senior Policy Counsel
Demand Progress Education Fund