COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER and THE AMERICAN CIVIL LIBERTIES UNION

to the

National Institute of Standards and Technology

on

Digital Identity Guidelines: Enrollment and Identity Proofing, Initial Public Draft

NIST SP 800-63A-4 ipd

April 14, 2023

The Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) submit these comments in response to the National Institute of Standards and Technologies' (NIST) draft Digital Identity Guidelines for Enrollment and Identity Proofing.[1] The updated guidelines provide technical standards for three levels of "identity assurance" to be used across the federal government and for the first time explicitly incorporates equity concerns.

EPIC is a public interest research center in Washington, DC established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC works to protect privacy by advocating for strong, privacy protective standards when individuals interact with government agencies, including identity verification.[2]

---

[1] Available at: https://csrc.nist.gov/publications/detail/sp/800-63/4/draft.

[2] *See e.g.* EPIC, Coalition Comments to DHS on Advance Passenger Information System: Electronic Validation of Travel Documents (Apr. 3, 2023), https://epic.org/wp-content/uploads/2023/04/IDP-APIS-comments-3APR2023.pdf; EPIC Comments to OSTP on Digital Assets Request for Information (Mar. 6, 2023), https://epic.org/documents/comments-of-epic-to-ostp-on-digital-assets-request-for-information/; EPIC Comments to GSA on Fraud Controls on Login.gov (Dec. 21, 2022), https://epic.org/documents/epic-comments-modified-system-of-records-notice-for-login-gov/; EPIC Spotlights Pondera's Fraud Detection

For more than 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

As was laid bare during the COVID-19 pandemic, identity verification systems that fail to properly address equity concerns can create potentially insurmountable barriers to people accessing essential government services. During the height of the pandemic, state workforce agencies rapidly adopted ID.me's identity verification system, purportedly NIST SP 800-63 IAL2 compliant, without providing for meaningful alternatives, requiring unemployment insurance applicants to upload government documents and snap selfies for facial recognition comparison or wait in hours-long online queues for trusted referees when automated processes failed.[3] For the many people who are on the wrong side of the digital divide --disproportionately Black, Latinx, Indiginous people and those with disabilities and/or rural households – and who lacked access to smartphones with cameras, reliable internet service, or who simply were less familiar with how to use a complex technology, the adoption of ID.me resulted in an inability to access government benefits when they needed them the most.[4] Moreover, facial recognition technology generally has differential error rates by race and

Algorithms for Public Benefits (Jul. 5, 2022), https://epic.org/epic-spotlights-ponderas-fraud-detection-algorithms-for-public-benefits/.

[3] Select Subcommittee on the Coronavirus Crisis, *Chairs Clyburn, Maloney Release Evidence Facial Recognition Company ID.me Downplayed Excessive Wait Times for Americans Seeking Unemployment Relief Funds*, U.S. House of Representatives (Nov. 17, 2022), https://oversightdemocrats.house.gov/news/press-releases/chairs-maloney-clyburn-release-evidence-facial-recognition-company-idme.

[4] Corin Faife, *Feds are still using ID.me to scan your face — and its human reviewers can't keep up*, The Verge (Feb. 11, 2022), https://www.theverge.com/2022/2/11/22928082/id-me-irs-facial-recognition-overworked-employees.

gender, further exacerbating the potential disparate impact of digital identity verification systems that employ it.

We urge NIST to modify the draft guidelines to 1) depreciate repeat, remote collections of biometric information, 2) remove the social security number as a valid attribute for identity verification and invest in alternatives 3) evaluate W3C Verifiable Credentials as a technical standard to improve remote identity verification, 4) target fraud prevention controls towards large-scale attacks and de-prioritize fraud prevention that creates barriers to claiming benefits, and 5) to further strengthen steps to address equity concerns by requiring agencies to provide multiple options for identity verification and other measures.

Background

NIST's Digital Identity Guidelines provide federal agencies with voluntary technical standards and systems for when an agency wants to confirm that an individual is who they say they are. That process is called "identity proofing." Identity proofing is substantially more complex in the remote/online context because verification requires proof that a) there is a real person behind the computer and b) that the credentials presented remotely are valid. NIST provides for three Identity Assurance Levels (IALs) corresponding with the level of confidence required by the agency. Each IAL comes with a set of technical standards and recommended processes. State agencies also consult NIST's Guidelines, so the process NIST sets out for determining the right identity assurance level and the standards NIST suggests have a widespread impact on identity proofing in the U.S. In the latest version of the Guidelines, NIST makes several substantial changes to the Institute's overall approach to identity proofing in order to promote systems that are more equitable, less dependent on face recognition, and more resilient against fraud.

First, NIST introduces the goal to "Advance Equity" in risk management and specifically instructs agencies to account for the impact of identity proofing processes "to individuals and

communities … including challenges to providing services to all people who are eligible for and entitled to them".[5] The equity considerations NIST proposes include requiring trusted referees and allowing for applicant references to vouch for individuals who lack certain documents, requiring equity assessments, and providing alternative infrastructure for individuals excluded by biometric systems.[6] This is an important step in the right direction.

Second, NIST seeks to "Emphasize Optionality and Choice for Consumers" by providing alternatives to identity proofing methods that require facial recognition technology.[7] As the leading experts on bias and error in facial recognition systems, NIST is well positioned to recognize the myriad harms from facial recognition technology.[8] NIST's decision to provide for for alternatives for facial recognition and endorse "the need for digital identity services to support multiple authenticator options" is also a meaningful step towards accounting for those harms and improving access to government benefits.

Third, NIST aims to introduce new fraud prevention measures and update its risk assessments to account for new forms of cyber attacks.[9] This includes for the first time considering accepting mobile drivers licenses or verifiable credentials for identity proofing.[10] NIST also approves new anti-phishing tools and automated attack prevention tools like bot detection, behavioral

[5] NIST SP 800-63A-4 ipd at ii.
[6] *Id*. at 51-55.
[7] *Id*. at ii.
[8] *See generally*, NIST Facial Recognition Vendor Tests (FVRT), https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt; New Jersey v. Arteaga N0. A-3078-21T1, brief of EPIC, EFF, and NACDL as amici curie, https://epic.org/documents/new-jersey-v-arteaga/; ACLU v. Clearview AI (settled), https://www.aclu.org/cases/aclu-v-clearview-ai; Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown Law Center on Privacy and Technology (Dec. 6, 2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.
[9] NIST SP 800-63A-4 ipd at ii.
[10] *Id*. at iii.

analytics, and traffic analysis.[11] Finally, NIST undertakes general updates to the identity assurance levels, federation assurance levels, and other changes.

I. NIST should depreciate repeat, remote collection of biometric data for identity proofing.

The draft guidelines take the first steps reducing the collection of biometric information by making it optional for IAL2, which is widely used across the federal government. It is important for NIST's draft guidelines to counsel agencies against remote facial recognition systems for several reasons. First, NIST is rightly concerned with the use of facial recognition techniques, which have been shown to generate biased results, making government identity proofing systems inequitable. Second, biometrics are poised to become increasingly weak guarantors of identity as the development of artificial intelligence makes it easier to spoof systems. NIST should embrace a strategy that moves away from remote and repeat biometric collection in favor of on-device biometric verification and robust in-person or live-help alternatives.

a. Biometrics are likely to become an increasingly weak form of identity verification.

Machine learning and generative AI are quickly creating a world where spoofing face and voice biometrics will be all too easy. The presence of these technologies requires escalating countermeasures, like the rapid spread of facial liveness testing, that increase barriers for individuals to access services.

Generative AI is already causing problems with fake images that are difficult to identify and voice imposters. Recently, a deepfake image of Pope Francis in a full-length Balenciaga puffy coat made news internationally for its realistic feel.[12] The celebrity deepfakes trend underscores a growing threat vector for digital identity fraud, using generative AI to fake identity. In 2021, a study

[11] *Id*. at 26.
[12] *See e.g.* Kalley Huang, *Why Pope Francis Is the Star of A.I.-Generated Photos*, N.Y. Times (Apr. 8, 2023),

found that common deepfake methods called generative adversarial networks (GANs) could trick advanced facial recognition systems. In the study, deepfakes were able to pass facial recognition systems 85 to 95 percent of the time.[13] As generative AI improves, facial recognition will become increasingly susceptible to attack, suggesting that using facial recognition as the basis for remote identity verification is not a sustainable practice.

Voice biometrics are subject to similar, even simpler attacks. Earlier this year, journalist Joseph Cox was able to break into his own bank account using an AI-generated voiceprint.[14] Another journalist was able to fool an Australian government agency voiceprint system with generative AI earlier this year.[15] And while voiceprints do not play a role in most current federal identity proofing, at least some agencies are exploring voiceprint identification. ICE's Alternatives to Detention program uses voiceprint recognition to verify the identity of migrants enrolled during regular check ins.[16] Outside of the federal government, voiceprint verification has spread rapidly in the last few years, especially in the banking industry.[17] Lawsuits over non-consensual use of voiceprint verification have also multiplied.[18] NIST should be aware of the trend in voiceprint biometrics and proactively engage to counsel agencies to avoid voiceprint biometrics.

---

[13] *Id*.
[14] Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.
[15] Nick Evershed and Josh Taylor, *AI can fool voice recognition used to verify identity by Centrelink and Australian tax office*, The Guardian (Mar. 16, 2023), https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai.
[16] DHS, DHS/ICE/PIA-062 Privacy Impact Assessment for the Alternatives to Detention (ATD) Program at 12-13v(Mar. 17, 2023), https://www.dhs.gov/sites/default/files/2023-03/privacy-pia-ice062-atd-march2023_1.pdf.
[17] Samantha Hawkins, *'Voiceprints' Roil Companies as Biometrics Litigation Skyrockets*, Bloomberg Law (May 18, 2022), https://news.bloomberglaw.com/privacy-and-data-security/voiceprints-roil-companies-as-biometrics-litigation-skyrockets; Jennifer A. Kingston, *Biometrics invade banking and retail*, Axios (Feb. 18, 2020), https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy.
[18] *Id*.

Existing weaknesses in facial recognition have pushed identity verification providers to institute facial liveness testing in addition to facial recognition. But facial liveness is an untested technology with no existing standards and has not been subjected to bias testing comparable to NIST's FRVT testing for facial recognition. At least some facial liveness products appear to have demonstrable biases, struggling to identify Black and Indigenous faces. The CBP One app rolled out for asylum seekers on the southern border includes a facial liveness test. Both migrants and immigrant-rights workers have documented a higher error rate for Black and Indigenous faces, especially when used in non-ideal lighting conditions.[19] Both Id.me and CBP One use iProov's facial liveness testing.[20]

The rise of facial liveness demonstrates that biometric verification will become increasingly complex and may end up in an arms race between new biometric technologies and generative AI spoofs. Such a race is not compatible with good government policy because constantly updating standards to introduce new technologies alienates users and creates additional barriers to access services. Similarly, introducing new and untested technologies will always create the risks of bias and error in new systems. Remote, repeat biometric collection is not a good future-proof model for identity verification.

b. Biometric collection enables more comprehensive surveillance.

The unnecessary expansion of biometric collection and use can lead to the loss of individual rights and freedoms. For example, the expansion of certain modalities, like DNA testing and facial recognition services, can cause increased risks of oppression and exploitation.[21] A person's right to

[19] John Washington, *Glitchy CBP One app turning volunteers into Geek Squad support for asylum-seekers in Nogales*, AZ Luminaria (Mar. 20, 2023), https://azluminaria.org/2023/03/20/glitchy-cbp-one-app-turning-volunteers-into-geek-squad-support-for-asylum-seekers-in-nogales/.
[20] *See generally*, iProov, Government and Public Sector, iproov.com (last accessed Apr. 10, 2023), https://www.iproov.com/what-we-do/industries/government-and-public-sector.
[21] Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

privacy, even in public spaces, is protected by the First and Fourth Amendment.[22] The more biometric information is collected, and exposed to government abuse or data breach, the less privacy individuals will have in public. NIST's steps to make biometric verification option for IAL2 are an important start towards a better identity system that will not enable more surveillance.

II. NIST should further depreciate the SSN as an acceptable attribute for identity verification.

The draft guidance, in line with years of federal policy, depreciates the practice of collecting Social Security Numbers (SSNs) or using them as proof of identity. Current OMB guidance and White House policy dating back to 2007 both instruct federal agencies to minimize collection and storage of SSNs. However, the current guidance § 8.1.1 continues to allow the collection of SSNs for identity proofing. NIST suggests valid pragmatic steps to reduce the risk of identity theft when agencies store SSN data, and rightly identifies that storing SSNs on third-party systems is a high-risk behavior. And yet, using the SSN is unfortunately still commonplace among many agencies' identity proofing processes. NIST's guidance should not accept the SSN as a valid attribute for identity verification. NIST should take further steps to move agencies away from collecting SSNs as part of the identity proofing process by proposing standards and systems that use individual agency identification numbers.

The SSN is a weak signifier of identity, and using the SSN in identity proofing creates substantial risks of fraud and identity theft. Data breaches involving SSNs are so common that the SSN has lost much of its value as a signifier that the person providing their social security number is not an imposter. The 2017 Equifax data breach alone exposed the SSNs of more than 145 million Americans.[23] For years, security experts have warned that virtually every person with a SSN has had

[22] *Id*.
[23] GAO-18-559, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach at 18-19 (Aug. 2018), https://www.gao.gov/assets/gao-18-559.pdf.

their number compromised at least once, and that everyone should act as if their SSN has been stolen.[24] The federal government recognized as early as 2007 that agencies collecting SSNs posed a threat and specifically instructed agencies to a) eliminate unnecessary use of SSNs and b) explore alternatives to the SSN.[25]

However, agencies have not made enough progress in reducing or eliminating use of the SSN to validate identity. In 2017 the Government Accountability Office (GAO) surveyed federal agencies collecting SSNs, finding that 22 agencies used the SSN in the provision of benefits and services.[26] The GAO issued five recommendations to the Office of Management and Budget to harmonize federal policy and meaningfully reduce how often agencies collect SSNs. As of 2021, OMB could not confirm that it had implemented any of the GAO's recommendations.[27] In short, agencies are repeatedly failing to act to remove the SSN from identity proofing. NIST can play a substantial role in remedying that failure and should act through these guidelines to remove the SSN as a valid form of identity verification.

NIST should consider unique agency-issued identifiers and other alternatives to the SSN. DHS's Science and Technology Directorate is already engaged in developing technology for the agency to issue "a globally unique, meaningless and verifiable identifier to be issued to

[24] Suzanne Rowan Kelleher, *Everyone's Social Security Number Has Been Compromised. Here's How To Protect Yourself*, Forbes (Aug. 1, 2019), https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=6ea189929ac7.
[25] OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf.
[26] GAO-17-553, Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display (Jul. 25, 2017), https://www.gao.gov/products/gao-17-553.
[27] *Id*.

individuals."[28] A unique agency identifier would reduce the potential harms caused by a data breach, preventing identity theft. The same technology could also limit the potential for surveillance within the federal government and provide individuals more privacy when applying for benefits.

III. NIST should evaluate W3C Verifiable Credentials for remote identity verification.

The Draft Guidelines ask about the potential for mobile drivers' licenses or verifiable credentials in remote identity verification.

The federal government does not have any universal standard for asserting a digital identity in place today. The two most commonly discussed digital identity standards are ISO/IEC mobile drivers licenses (mDLs)[29] and W3C Verifiable Credentials (VCs).[30] If NIST endorses a technical standard for remote identity verification, that standard should provide the individual with the greatest possible control over their information and the most robust privacy protections. EPIC and the ACLU recommend that NIST rigorously review the W3C Verifiable Credentials standard to determine if the standard is a good fit for agencies' identity verification needs and to ensure that the standard adequately protects privacy.

Currently, different components within the Department of Homeland Security (DHS) are working on implementing both mDLs and Verifiable Credentials in different applications. The Transportation Security Administration (TSA) is currently piloting mDLs issued by several states at select checkpoints in the U.S.[31] Meanwhile U.S. Citizenship and Immigration Services, another DHS

---

[28] DHS, *News Release: DHS Awards $193K for a Standards Based Approach to an Alternative Identifier to the Social Security Number* (Oct. 9, 2020), https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-awards-alternative-identifier-social-security-number.
[29] ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (Sept. 2021), https://www.iso.org/standard/69084.html.
[30] W3C Recommendation Verifiable Credentials Data Model v1.1 (Mar. 3, 2022), https://www.w3.org/TR/vc-data-model/.
[31] TSA, *When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology?*, tsa.gov (last accessed Apr. 8, 2023), https://www.tsa.gov/travel/frequently-asked-questions/when-will-phased-digital-id-rollout-start-which-airportsstates,

component, is developing a digital version of green cards enabled by W3C Verifiable Credentials.[32] For more on the promise and potential flaws with digital credentials, see the ACLU's report on Digital Drivers' Licenses.[33]

Further, the best design for a universal digital identity system would allow for privacy-preserving authentication, i.e. would be compatible with anonymous credentials. [34] W3C Verifiable Credentials are compatible with anonymous credentialing. Anonymous credentials would, for example, allow a federal employee to convince a verifier that the employee has a security clearance, without revealing any other information. The same system would allow someone presenting a mobile drivers' license at a liquor store to transmit only the information that the person is over the age of 21, and eligible to buy alcohol. In particular, anonymous credentials would prevent the identification from leaving behind a persistent identifier that would allow to link the individual to another authentication instance. This both safeguards the personal privacy of the person (so that even prying verifiers cannot trace this employee across many transactions) and in government applications, protects the government's secrets.

[32] DHS Science and Technology Directorate, DHS Implementation Profile of W3C VCs and W3C DIDs (presentation), W3 (Sept. 29, 2022), https://lists.w3.org/Archives/Public/public-credentials/2022Sep/att-0253/DHS.W3C.VC-DID.Implemenation.Profile-20220929-SHARE.pdf.

[33] Jay Stanley, *Identity Crisis What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom, ACLU* (May 2021), https://www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom,

[34] *See e.g.* Anna Lysyanskya, *Signature schemes and applications to cryptographic protocol design* (2002), https://dspace.mit.edu/handle/1721.1/29271, Melissa Chase, *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications* (May 2008), http://static.cs.brown.edu/research/pubs/theses/phd/2008/chase.pdf, Fonteini Baldimtsi, *Efficient Cryptography for Information Privacy* (May 2014), https://cs.brown.edu/research/pubs/theses/phd/2014/baldimtsi.pdf, Endre Bangerter, Jan Camenisch, Anna Lysyanskaya, *A Cryptographic Framework for the Controlled Release of Certified Data*, 3957 LNCS 20-42 (2006), https://link.springer.com/chapter/10.1007%2F11861386_4.

IV. NIST should limit fraud prevention to addressing large-scale attacks and specifically avoid tools that impose high barriers to claiming benefits.

The Draft Guidelines request feedback on both fraud checks and fraud prevention techniques, including questions about fraud analytics, risk scoring, and privacy and equity concerns.[35]

Fraud prevention is an important element of any identity proofing scheme, but frequently poses an unnecessary barrier to individuals claiming benefits. The harms of poorly designed fraud prevention technologies fall hardest upon marginalized groups including Black and Brown communities, immigrants, low-income individuals, the elderly, and people living in rural areas. The touchstone for fraud prevention tools should be equity. Tools that exhibit bias or a propensity for error should not be used, even if they claim to be highly effective. As a baseline rule, fraud prevention tools targeted at catching large scale attacks are less likely to harm individuals than tools for risk-scoring and back-end matching programs. NIST should also be careful to analyze any behavioral analysis tools for privacy risks and equity concerns.

Behavioral analysis for online fraud monitoring is one tool that NIST should study intensively before suggesting as an option, much less requiring for identity proofing. Such analysis has the potential to become behavioral surveillance. Tracking how individuals use computers risks revealing users' medical information. At least one study used mouse movements to identify mild cognitive impairments associated with Alzheimer's disease as an early diagnosis tool.[36] Behavioral monitoring is also likely to capture information about individuals with disabilities, including people who are blind, individuals with limited vision, and those with neuromuscular conditions. For example, mouse movements have been used to screen for Parkinson's disease and similar

[35] Draft Guidelines at iii.
[36] Adriana Seelye et al., *Computer mouse movement patterns: A potential marker of mild cognitive impairment*, Alzheimers Dement (Amst.) 472-80 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4748737/.

conditions.[37] Internet users with disabilities may also be disproportionately flagged by poorly designed fraud monitoring tools because their behavioral patterns will differ from abled users. Behavioral analysis creates an additional risk of harm that must be accounted for. For the federal government, behavioral analysis is often run through third-party contractors like LexisNexis, creating more privacy concerns when data is housed in multiple locations and made available to data brokers.[38]

Finally, risk scoring by algorithm is prone to errors and bias that must be accounted for. NIST should clearly articulate that risk scoring is not a technology ready for prime-time, and that algorithmic risk scoring may never be sufficiently unbiased to be worth the risk. Rigorous algorithmic impact assessments can detect the presence of bias and likelihood for errors, but not eliminate them. For a thorough treatment of the harms associated with algorithmic scoring, see EPIC's Screening and Scoring Project[39] and our recent report, *Screened and Scored in D.C.*[40]

NIST should subject any scoring algorithms, internal or external, to an intensive algorithmic impact assessment and provide an avenue of appeal when accounts are flagged as fraudulent. If an account is flagged but individuals do not understand why they are denied access to government websites and given a means to appeal, the government risks preventing individuals access to vital government benefits and entrenching discriminatory patterns.

Moreover, at minimum, NIST should revise the Draft Guidelines to require equity assessments for fraud mitigation measures. The draft framework states that where CSPs chooses to

---

[37] Kryzstof Gajos et al., *Computer Mouse Use Captures Ataxia and Parkinsonism, Enabling Accurate Measurement and Detection*, Wiley InterScience (Jul. 8, 2019), https://movementdisorders.onlinelibrary.wiley.com/doi/10.1002/mds.27915.
[38] *See* EPIC Comments to the GSA on Login.gov (Dec. 21, 2022), https://epic.org/documents/epic-comments-modified-system-of-records-notice-for-login-gov/.
[39] https://epic.org/issues/ai/screening-scoring/.
[40] Thomas McBrien et al., *Screened and Scored in the District of Columbia*, EPIC (Nov. 2022), https://epic.org/screened-scored-in-dc/.

employ fraud mitigation measures such as "examining the device characteristics of the applicant [and] evaluating behavioral characteristics", they must conduct a privacy risk assessment for such measures.[41] NIST should also require equity assessments for fraud mitigation measures. To the extent that fraud mitigation measures are based on discriminatory data and assumptions, there is an enormous danger that legitimate claimants from marginalized communities will be incorrectly flagged for fraud.

V. NIST should take stronger steps to address equity.

EPIC and the ACLU wholeheartedly support NIST's incorporation of equity considerations into its draft digital identity framework, including through mandating assessments of potential inequity in "access, treatment, or outcomes" as part of the risk assessment process (800-63A-4 sec 5.1.3); requiring adherence to minimum performance metrics of biometric systems, including similarity of performance across different demographic groups, and independent, publicly available assessments of systems in conditions similar to real world uses (800-63A-4 sec 5.1.8); and adopting options for remote identity proofing at Identity Assurance Level 2 that do not involve facial recognition (800-63A-4 sec 5.4.4.1).

It is also a critical step forward that NIST's proposal includes requiring consideration of privacy, equity and usability in selecting assurance levels (800-63-4 section 5), as there is a risk that agencies will begin to default to the most strict levels of assurance. A lower assurance level or even forgoing strict identity verification protocols may be appropriate for a host of online interactions, and government agencies must be mindful of balancing any legitimate concerns about fraud with the need to ensure timely and meaningful access to services and benefits for eligible individuals.

[41] NIST SP 800-63A-4 ipd at sec 5.1.1.2.

EPIC and the ACLU provide the following recommendations for further strengthening the equity protections in NIST's draft digital identity framework:

a. Optionality should be mandatory, not just recommended.

In its "Note to Reviewers," NIST states that the "draft seeks to…Emphasize Optionality and Choice for Consumers." Optionality is critical to ensuring accessibility and equity, as solutions that may increase accessibility for some people may be less accessible for others. Yet the draft does not mandate that CSPs and organizations provide people options for methods to verify their identity, and instead merely state that "[t]o the extent practical, CSPs and organizations SHOULD enable optionality." (800-63-4 and 800-63A-4, sec 4). Given the importance of optionality to promoting "access for those with different means, capabilities, and technology access," id., NIST should revise the framework to state that CSPs and organizations "SHALL" provide for optionality.

b. Clarify the need to directly consult with impacted individuals and communities in assessing equity.

The draft helpfully includes numerous stages at which potential disparities and harms to individuals must be considered, from assurance level selection and system design through reassessments after implementation. The framework does not, however, provide sufficient clarity as to how such disparities and harms may be identified, and critically fails to mandate or even sufficiently encourage consultation with the individuals and communities that will be using these systems, the people who have the greatest expertise in identifying the ways that these systems can fail. NIST should make clear that CSPs and organizations must engage with impacted communities and users in order to effectively identify potential barriers and harms as well as possible solutions.

c. Clarify rules around expired documentation for fair evidence.

The draft provides that fair evidence can include documentation that has expired within the last 6 months, yet elsewhere, the draft states that "[e]vidence at all levels of strength must be current

and unexpired." (Compare 800-63A-4 section 4.3.3 with 4.3.3.1). Flexibility in allowing for the use of expired documentation is useful in increasing accessibility, as various systemic inequities such as burdensome and expensive documentation requirements can create disparities in who is able to maintain updated documentation.[42] NIST should clarify that fair evidence includes recently expired documentation and should consider expanding the ability to use expired documentation as evidence of identity. Maintaining up-to-date drivers' licenses and passports requires time and resources that poor and marginalized communities are less likely to possess. NIST should recognize that requiring unexpired documentation creates a burden that will fall more heavily on marginalized communities and does not provide substantial benefits for security or confidence in identity verification.

d. *Clarify that agencies relying on third-party CSPs must conduct their own equity assessments*.

Where agencies use a third-party CSP, the framework states that "the agency SHALL be responsible for conducting its own privacy risk assessments or doing due diligence before relying on the CSP's privacy risk assessment as part of its PIA process," but agencies "SHALL incorporate the CSP's assessment of equity risks into its own assessment of equity risks" (800-63A-4 sec. 5.1.5.8-9). This formulation makes it unclear to what extent agencies are required to do their own due diligence with respect to equity. NIST should make clear that while agencies should require CSPs to conduct equity assessments, agencies themselves have an obligation to assess equity harms and conduct due diligence on third party equity assessments.

e. *Require that performance metrics be broken down by demographics.*

NIST has required that face recognition algorithms meet certain performance metrics — that only one in 10,000 comparisons result in a false match, and that only one in 100 comparisons result

[42] Movement Advancement Project, *The ID Divide: How Barriers to ID Impact Different Communities and Affect Us All* (Nov, 2022), https://www.mapresearch.org/file/MAP-Identity-Documents-report-2022.pdf.

in a false non-match.[43] These lopsided benchmarks would institutionalize a prioritization of security interests over the interest in not creating access barriers for individuals who are falsely non-matched. In addition, NIST should require that performance metrics be broken down by demographics, and not solely the population as a whole, which risks hiding demographic differentials in false matches and non-matches.

[43] Page 23, Lines 935-937

Conclusion

EPIC and the ACLU applaud NIST's leadership in publishing guidelines on digital identity that are a crucial resource for government agencies implementing identity verification systems. 1) depreciate repeat, remote collections of biometric information, 2) remove the social security number as a valid attribute for identity verification and invest in alternatives 3) evaluate W3C Verifiable Credentials as a technical standard to improve remote identity verification, 4) target fraud prevention controls towards large-scale attacks and de-prioritize fraud prevention that creates barriers to claiming benefit, and 5) to further strengthen steps to address equity concerns by requiring agencies to provide multiple options for identity verification and other measures. For further questions, please contact EPIC Counsel Jake Wiener at wiener@epic.org and ACLU Senior Policy Analyst Jay Stanley at jstanley@aclu.org or Olga Akselrod, ACLU Senior Staff Attorney at oakselrod@aclu.org.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Counsel

Jay Stanley
Jay Stanley
ACLU Senior Policy Analyst

Alan Butler
Alan Butler
EPIC Executive Director

Olga Akselrod
Olga Akselrod
ACLU Senior Staff Attorney