Comments of the

AMERICAN CIVIL LIBERTIES UNION

and the

ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Digital Identity Guidelines: Second Public Draft
NIST SP 800-63 Revision 4 & Companion Publications

October 7, 2024

TABLE OF CONTENTS

ACLU and EPIC

The American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) submit these comments in response to the National Institute of Standards and Technology's (NIST's) Request for Comment on NIST's Second Public Draft of Digital Identity Guidelines.[1] These comments are a continuation of comments submitted by the ACLU and EPIC in response to the Initial Public Draft of NIST's Digital Identity Draft Guidelines last year.[2]

For more than 100 years, the ACLU has been our nation's guardian of liberty and equality, 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, and conducts advocacy and litigation aimed at ending discrimination in all its forms, including at the intersection of technology and civil rights. 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.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long worked to protect privacy by advocating for strong, privacy protective standards for the collection, use, and retention of personal information, including efforts to support robust technical safeguards like data de-identification,[3] differential privacy,[4] and other privacy-enhancing techniques.[5] Over the last several years, EPIC has repeatedly intervened in support of

[1] Press Release, NIST, NIST Releases Second Public Draft of Digital Identity Guidelines for Final Review (Aug. 21, 2024), https://www.nist.gov/news-events/news/2024/08/nist-releases-second-public-draft-digital-identity-guidelines-final-review.
[2] ACLU & EPIC, Comments on NIST's 2023 Digital Identity Draft Guidelines (Apr. 14, 2023), https://epic.org/documents/epic-and-aclu-comments-on-nists-2023-digital-identity-draft-guidelines/ [hereinafter "Joint Comments on the Initial Public Draft"].
[3] EPIC, Comments on NIST's De-Identifying Government Data Sets Paper (Jan. 13, 2023), https://epic.org/documents/epic-comments-on-nist-de-identifying-government-data-sets-paper-3rd-draft/.
[4] *See Census Privacy*, EPIC (2022), https://epic.org/issues/democracy-free-speech/census-privacy/.
[5] EPIC, Comments to OSTP on Advancing Differential Privacy (July 8, 2022), https://epic.org/documents/epic-comments-to-ostp-on-advancing-differential-privacy/.

more privacy- and consumer-protective procedures when individuals interact with government agencies, including for fraud detection[6] and identity verification.[7]

INTRODUCTION

Across private and public sectors, digital identity services depend on trust. And trust, in this instance, depends not only on an identity holder's *understanding* of the digital identity process, but also on how *equitable* the process is. Automated identity verification systems, without proper testing and fine-tuning, can produce unreliable—even biased—results. Processes without sufficient optionality and community engagement can create insurmountable barriers to those most in need. And guidance that enshrines unreliable identity attributes and identity verification processes makes digital identity services more vulnerable, not less, to fraud and errors.

In April 2023, the ACLU and EPIC urged NIST to consider five key concerns relating to the Initial Public Draft of NIST's Digital Identity Draft Guidelines. **First,** digital identity services that rely on remote, unattended facial recognition and other biometric systems are unreliable due to the inherent biases present in current facial recognition technologies—as well as the increasing sophistication of biometric spoofing techniques using generative artificial intelligence.[8] **Second,** the Social Security Number has become an unreliable signifier of identity due to the frequency of data breaches involving SSNs.[9] **Third**, endorsing a technical standard for remotely asserting digital identity, without proper data controls and privacy protections, may increase the risks of digital identity services rather than decrease them.[10] **Fourth**, digital identity and fraud prevention techniques can impose serious barriers to individuals seeking benefits or other assistance, so any

---

[6] *See, e.g.*, Complaint, Request for Investigation, Injunction, and Other Relief, *In re Thomson Reuters* (Jan. 4, 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-FTC-Thomson-Reuters-Complaint.pdf.

[7] *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-APIScomments-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/epiccomments-modified-system-of-records-notice-for-login-gov/; *EPIC Screening and Scoring Spotlight: Pondera's Fraud Prediction Algorithms for Public Benefits*, EPIC, https://epic.org/pondera-surveillance/ (last visited Sept. 27, 2024).

[8] Joint Comments on the Initial Public Draft at 5–8; *see also* Kalley Huang, *Why Pope Francis Is the Star of A.I.-Generated Photos*, N.Y. Times (Apr. 8, 2023), https://www.nytimes.com/2023/04/08/technology/ai-photos-pope-francis.html; Nick Evershed & 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.

[9] Joint Comments on the Initial Public Draft at 8–10.

[10] *Id.* at 10–11.

digital identity guidelines should focus predominantly on efforts to prevent large-scale attacks.[11] And **fifth**, equity and accessibility considerations must be at the core of any digital identity guidelines—including the need for greater optionality and choice for consumers interacting with digital identity services.[12]

In this comment, EPIC and the ACLU provide updated recommendations intended to fortify NIST's existing identity protections while expanding the accessibility and equity of digital identity services. We believe NIST's Digital Identity Guidelines can foster crucial public trust in digital identity services and the programs they serve, and we applaud NIST for the crucial steps it has already taken—through the publication of the Second Public Draft Digital Identity Guidelines—to increase trust, reliability, security, and accessibility within digital identity services. For example, NIST now requires credential service providers (CSPs) to always offer, at minimum, two options for identity proofing: unattended remote identity proofing and remote or onsite attended identity proofing.[13] As noted in our April 2023 Comments on the Initial Public Draft, optionality is critical to ensuring accessibility and equity, since services that increase accessibility for some people may decrease accessibility for others.[14] Additionally, NIST's adoption of guidelines involving attribute bundles and digital wallets evinces a strong, albeit incomplete, step toward more robust, universal, and privacy-protective technical standards for remote identity verification.

Without additional normative safeguards in place, however, NIST's Digital Identity Guidelines will fall short of the agency's goal of enabling the "implementation of secure, private, equitable, and accessible identity systems."[15] In particular, EPIC and the ACLU urge NIST to:

1. Refocus fraud management guidance around large-scale, organized fraud schemes;

2. Depreciate services that rely on third-party service providers or foster second-order risks within the private sector;

3. Strengthen the Guidelines to promote greater equity, including by:

    a. Requiring an in-person identity verification option;
    b. Mandating consultations with impacted individuals or communities and civil society when developing and implementing digital identity services;

[11] *Id.* at 12–14.
[12] *Id.* at 14–17.
[13] SP 800-63A-4 at 36.
[14] Joint Comments on the Initial Public Draft at 15.
[15] *Id.* at ii.

c. Requiring both CSPs and relying parties (RPs) to perform equity assessments and ongoing monitoring for fraud mitigation measures; and
d. Further clarify the validity of expired documentation for identity verification purposes.

4. Further emphasize anonymous and pseudonymous authorization mechanisms; and

5. Rethink the user groups model.

Below, the ACLU and EPIC have provided more granular recommendations to support the need for these additional changes.

I. NIST SHOULD REFOCUS FRAUD MANAGEMENT GUIDANCE AROUND LARGE-SCALE, ORGANIZED ATTACKS

Any technical or procedural standard for digital identity verification will require implementing additional hinge points within the identity verification process: who can access services, from where, and with what documentation? How many steps must an individual complete to accomplish identity resolution, validation, and verification—and how long do those steps take? And how quickly are issues involving errors or fraud resolved? All these questions impose risks to equity, privacy, and accessibility for individuals who must navigate digital identity services to access crucial benefits or assistance. Therefore, to effectively implement digital identity guidelines, EPIC and the ACLU reemphasize the need to focus fraud prevention provisions within NIST's Digital Identity Guidelines on large-scale, organized attacks while avoiding tools that impose undue barriers to legitimate claimants seeking benefits or assistance.

As stated in our April 2023 Joint Comments on the Initial Public Draft, fraud management and prevention can impose serious and unnecessary barriers to individuals legitimately claiming benefits. Risk scoring tools can inject errors and biases into identity verification and fraud detection—often in ways that are difficult for claimants and agencies alike to parse.[16] In one recent example, a Thomson Reuters fraud detection system used in California to screen unemployment insurance claimants for fraud incorrectly flagged 600,000 legitimate claimants as fraudulent

[16] *See* Grant Fergusson, EPIC, Outsourced & Automated 16–25 (2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf; Thomas McBrien et al., EPIC, Screened and Scored in the District of Columbia 11–16, 22–30 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf; *Screening & Scoring*, EPIC, https://epic.org/issues/ai/screening-scoring/ (last visited Oct. 3, 2024).

users—more than half of all claimants screened by the system.[17] Similarly, biometric and behavioral analytics tools used for remote fraud monitoring may improperly capture and retain user information, including sensitive health information. For example, mouse movements have been used to identify cognitive impairments and screen individuals for Parkinson's disease;[18] without proper oversight, similar behavioral tracking techniques may improperly flag claimants with disabilities as fraudulent users. And because many of these fraud management and detection systems are operated by third-party vendors like Thomson Reuters, LexisNexis, and Deloitte, sensitive user data collected by fraud detection systems can raise additional data privacy and security concerns as well.[19]

Currently, NIST's Second Public Draft views fraud management and prevention within digital identity systems expansively. For example, the Draft Guidelines currently mandate that "CSPs *shall* establish and maintain a fraud management program that provides fraud identification, detection, investigation, detection, investigation, reporting, and resolution capabilities," which extends to all applicants.[20] NIST further encourages CSPs to implement a broad range of additional fraud checks, including transaction analytics and fraud indicator checks,[21] that have been connected to faulty fraud determinations by existing fraud detection systems due to an overreliance on automated screening.[22]

Fraud detection and management is a core element of any effective identity proofing process, but NIST's endorsement of broad-based, individually targeted fraud detection across all applicants risks overestimating the relative risk and impact of individual fraudsters compared to large-scale, organized criminal fraud schemes. As reported by the U.S. Government Accountability Office in December 2022:

> "In its fiscal year 2020 Agency Financial Report, DOL acknowledged an increase in potentially fraudulent activity related to organized fraud schemes targeting the pandemic UI programs. Moreover, according to National Association of State Workforce Agencies (NASWA) officials, the UI system has faced unrelenting attacks by foreign organized crime groups during the pandemic. Also, in a March

[17] *See* Cal. Leg. Analyst's Off., Assessing Proposals to Address Unemployment Insurance Fraud (2022), https://perma.cc/98SC-LGYH.
[18] Joint Comments on the Initial Public Draft at 12–13.
[19] *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/.
[20] SP 800-63A-4 § 3.1.2.1.
[21] *Id.*
[22] *See* Cal. Leg. Analyst's Off., Assessing Proposals to Address Unemployment Insurance Fraud (2022), https://perma.cc/98SC-LGYH.

> 2021 press release, the U.S. Secret Service noted that its early investigation and analysis indicated that international organized criminal groups have targeted UI funds using stolen identities to file for UI benefits."[23]

Fraud prevention tools and techniques targeting large-scale, organized attacks are more likely to catch and remedy high-risk fraud and less likely to harm legitimate applicants than their broad-based counterparts, such as individualized risk scoring systems—especially when broad-based fraud management systems are supported by faulty algorithms. By refocusing language around fraud management toward large-scale, organized attacks, NIST can reduce the risk of equity and accessibility barriers within digital identity systems while maintaining high standards for fraud management.

II. NIST SHOULD ADDRESS SECOND-ORDER RISKS INVOLVING THIRD-PARTY VENDORS AND PRIVATE SECTOR USE

NIST's Digital Identity Guidelines will impact not only organizations deploying digital identity solutions today, but also the broader market for digital identity tools and services. Given the potential second-order impacts of this guidance, including broad influence over government contractors for digital identity solutions and private sector adoption of digital identity technologies, the ACLU and EPIC encourage NIST to carefully consider—and address—the second-order risks that its Digital Identity Guidelines will pose.

First, we recommend that NIST more closely consider second-order consequences of digital identity programs in the private sector. We are concerned that companies and other non-governmental entities will use and over-use a digital identity infrastructure once it is created. If an agency central to Americans' lives (like a DMV or tax authority, which people have little opportunity to disengage from) effectively requires engagement with some third-party identity providers (IdPs) or CSPs, and if those routes to identity proofing become commonplace and easy to use, then other would-be RPs can demand detailed authentication from all their customers with very little additional friction. That would facilitate a slide into a ubiquitous authentication environment, where engaging online anonymously is increasingly difficult, and individual activity, online and off, can be tracked by commercial actors, governments, and criminal actors alike. To counteract these second-order risks, NIST should encourage agencies to prefer adoption of systems that have mechanisms to curb abuse of authentication — such as systems that allow users to control

[23] GAO-23-105523 (internal citations omitted).

and minimize what data flows to RPs, identify those who are asking for their authentication, keep logs of authentication requests, and have meaningful redress policies against abusive authentication requests. NIST should discourage the use and urge agencies to abandon systems that offer no such protections or whose protections are found to be inadequate. To address these risks, NIST should encourage agencies' Senior Agency Officials for Privacy (SAOPs) to work closely with Chief Information Officers and Contracting Officers on the procurement and performance evaluation of any third-party vendors. NIST must also closely monitor the adoption of its Digital Identity Guidelines and update its guidance should private sector over-use foster unnecessary data collection beyond what is required for an appropriate IAL or undermine online privacy and anonymity in circumstances where no identity proofing is necessary. To encourage continued evaluation, NIST should encourage agency SAOPs monitor the application of authorized assurance levels for any emergent privacy or equity risks and encourage agencies to provide the public with a way to provide the agency with ongoing feedback on the service.

Second, we encourage NIST to carefully consider the risks inherent to third-party contracting within digital identity systems, especially for government use cases. Outsourcing core features of digital identity systems not only raises additional data privacy and security concerns, as private entities may collect, process, or retain applicant data in improper or unsecure ways, but also creates information gaps within a digital identity system that make it difficult for both government agencies and applicants to ensure digital identity systems are functioning properly.[24] For government agencies to properly adopt NIST's guidelines, they will need sufficient information about, control over, and training on all aspects of the digital identity systems they choose to implement.

These second-order risks are only exacerbated when government agencies contract with large data brokers and oligopolistic companies—as is the case for several public benefits programs around the country.[25] Consider the current market for digital wallets. Because Apple and Google control an overwhelming majority of the American smartphone market—where most consumers interact with digital wallet architecture—NIST's explicit focus on factors like "usability" [26] risks incentivizing agencies to work with major, pre-existing providers due to existing user adoption, even when better, more privacy protective options are available. A decision by an important government agency to further cement the technical dominance of these major service providers may undermine important innovation in privacy-protective digital identity technologies; such a

[24] Outsourced & Automated, *supra* note 16, at 11–25.
[25] *See* Outsourced & Automated, *supra* note 16, at 26–48, 68–124.
[26] *See* SP 800-63A-4 § 8.

result is not in the public interest. NIST can ameliorate this risk by ensuring that Free/Libre Open-Source Software wallets can be used with standards-based provisioning and presentation mechanisms. It should encourage the use of robust technical and policy-based safeguards that constrain and penalize abusive verifiers, while inducing appropriate friction during excessive requests for identification data.

III. NIST SHOULD FURTHER STRENGTHEN PROVISIONS TO ADDRESS EQUITY

As stated in our April 2023 Joint Comments on the Initial Public Draft, EPIC and the ACLU fully support NIST's inclusion of equity considerations in the framework for digital identity, including important requirements that NIST has retained in the Second Public Draft such as mandating assessments of potential inequity in "access, treatment, or outcomes" as part of the risk assessment process;[27] requiring adherence to minimum performance metrics for biometric systems, including similarity of performance across different demographic groups, and ongoing independent, publicly available assessments of systems in conditions similar to real world uses;[28] adopting options for remote identity proofing at Identity Assurance Level 2 that do not involve facial recognition;[29] and requiring consideration of privacy, equity and usability in selecting assurance levels.[30][31] Such steps are critical to ensuring that identity verification systems do not create potentially insurmountable barriers to essential services for people on the wrong side of the digital divide—disproportionately Black, Latine, Indigenous people and those with disabilities and/or rural households—and do not mandate facial recognition technology that generally has differential error rates by race and gender and raises additional privacy and equity risks.

While NIST addressed some of the additional recommendations we made in our April 2023 Comments, to further strengthen the equity protections in NIST's draft digital identity framework, we note here some remaining concerns and further recommendations:

A. Require a Meaningful In-Person Identity Verification Pathway

The Second Public Draft states that "CSPs and RPs SHALL provide options when implementing their identity proofing processes to promote access for applicants with different

[27] SP 800-63A-4 § 3.1.4.
[28] SP 800-63A-4 § 3.1.11.
[29] SP 800-63A-4 § 4.2.6.1–2.
[30] SP 800-63-4 § 3.4.1.
[31] Joint Comments on the Initial Public Draft at 14–15.

means, capabilities and technology access"[32] and recognizes that in-person options "can help ensure that those impacted by the digital divide are still able to access services offered by the CSP or RP."[33] But critically, the Second Public Draft does not mandate that CSPs or RPs provide an in-person pathway to identity verification. While the Draft requires CSPs to provide at least one attended process option for IAL1 or IAL2 in addition to a Remote Unattended process, CSPs can choose to provide an attended process that is solely remote and there is no requirement to provide an onsite process.[34]

The lack of a requirement for an in-person verification option is highly detrimental to ensuring that identity verification is widely accessible and equitable. Remote processes—whether unattended or attended—can be inaccessible for the many individuals who lack access to smartphones with cameras, reliable internet service, or who simply are less familiar with how to use complex technology. People should never be locked out of critical services because of a lack of technology to engage in identity verification processes. NIST should revise the draft to require CSPs to provide an onsite attended or unattended option, and to require RPs to provide a meaningful in person option.

B. Mandate Consultation with Impacted Individuals and Communities in Assessing Equity

In our Initial Comments, we recommended that NIST require CSPs and RPs to engage with the individuals and communities impacted by identity verification technologies—the people who have the greatest expertise in identifying the ways that these systems can fail—in order to assess equity considerations.[35] NIST has made some revisions that address that concern in the Second Public Draft, but the revisions are insufficient to ensure the consultation and feedback we recommended. In particular, the Second Public Draft adds a provision that "[o]rganizations SHOULD leverage consultation and feedback to ensure that the tailoring process addresses the constraints of the entities and communities served," but the provision is not mandatory and doesn't explicitly state that consultation and feedback should be directly with impacted individuals and communities. The Second Public Draft also states organizations "MAY" consult with civil society

[32] SP 800-63A-4 § 2. In our prior comments, we recommended that NIST should require CSPs and RPs to provide people with options for methods to verify their identity to ensure accessibility and equity, and to specifically revise the provision in the framework that "[t]o the extent practical, CSPs and organizations SHOULD enable optionality," Initial Public Draft 800-63-4 and 800-63A-4 § 4, to read that they "SHALL" enable optionality. Joint Comments on the Initial Public Draft at 15. The Second Public Draft now requires optionality. SP 800-63A-4 § 2.
[33] SP 800-63A-4 § 9.
[34] SP 800-63A-4 § 2.1.3.
[35] Joint Comments on the Initial Public Draft at 15.

organizations for input, instead of requiring that they do so.[36] NIST should revise the guidelines to make clear that CSPs and RPs "SHALL" engage both with impacted individuals and communities and with civil society organizations in order to effectively identify potential barriers and harms as well as possible solutions.

In addition, consideration of non-users should be increased. Non-users are both prospective users who declined to engage for some reason and people who might be affected by the given system even if they don't participate. In lines 1116 and 1117 of SP-800-63-4.2pd, user groups are identified as being mandatory to consider during impact assessments (SHALL), but affected non-users are only recommended for consideration (SHOULD). Consideration of non-user groups should be made mandatory as well.

C. Require Equity Assessment for Fraud Mitigation Measures

As discussed above, the Second Public Draft mandates that CSPs maintain a fraud management program.[37] Yet to the extent that fraud mitigation measures are based on discriminatory data and assumptions, there is an enormous danger that claimants who are Black, Latine, or Indigenous or from other marginalized communities will be incorrectly flagged for fraud. The Second Public Draft does not have sufficient provisions to ensure that anti-fraud programs do not wrongly ensnare or create barriers for legitimate claimants. NIST requires CSPs and RPs to perform a privacy assessment,[38] but neither are required to perform the equity assessments that NIST has required for identity verification processes as a whole. In addition, while CSPs are required to "continuously monitor the performance of their fraud checks and fraud mitigation technologies to identify and remediate issues related to disparate performance across their platforms or between the demographic groups,"[39] there are no such requirements for RPs. NIST should require both CSPs and RPs to perform equity assessments for fraud mitigation measures prior to their adoption to determine whether the measures can be used without disparately ensnaring legitimate Black and other applicants of color, and to conduct ongoing monitoring for disparities with requirements to mitigate or decommission fraud mitigation measures as needed.

Overall, the primacy and specificity of the anti-fraud concerns identified in the IAL, AAL, and FAL levels prioritize the security concerns of institutions over the privacy and equity evaluations, which have much more vague evaluation mechanisms and remediation proposals.

---

[36] SP 800-63-4 § 3.4.1.
[37] SP 800-63A-4 § 3.1.2.1.
[38] SP 800-63A-4 §§ 3.1.2.1(2), 3.1.2.2(5).
[39] SP 800-63A-4 § 3.1.2.1(10).

While it's good that they're at least identified as concerns, lower priority, less concrete goals will tend to be sidelined in favor of goals with specific, measurable targets. We recommend that NIST treat privacy and equity evaluations with the same weight and specificity as the security interests of institutions. To give privacy and equity the same weight as security, additional privacy and equity harms (such as a potential loss of opportunity to government services) should be documented in the Initial Impact Assessment stage of the Digital Identity Risk Management process and not exclusively in a fourth stage dedicated to tailoring assurance levels. This might take the form of concrete examples, specific targets, and documented evaluations of costs of privacy and equity failures to the organization, for example.

D. Clarify Rules Around Expired Documentation

In our initial comments, we recommended that NIST expand the ability to use expired documentation as evidence of identity because of the various systemic inequities that create disparities the ability to maintain unexpired documentation. In the Second Public Draft, NIST appears to have done so, noting that it replaced the term "expired" with "valid" "in recognition that evidence can remain a useful means to prove identity, even if it is expired or was issued outside a determined timeframe."[40] NIST also removed the requirement that evidence be "unexpired" from the requirements for fair, strong and superior evidence of identity.[41] However, the Second Public Draft still confusingly states that "validation involves examining the presented evidence to confirm it is … valid (unexpired or within the CSP's defined timeframe for issuance or expiration)."[42] NIST should clarify this provision to ensure CSPs and RPs understand that they can rely on expired evidence for identity verification.

[40] SP 800-63A-4 § 2.4.
[41] SP 800-63A-4 § 2.4.1.1–3.
[42] SP 800-63A-4 § 2.4.2.

IV. NIST Should Emphasize Anonymous and Pseudonymous Authorization Mechanisms

SP-800-63-4 focuses primarily on activity that involves full individualized authentication, and gives short shrift to less privacy-invasive, more anonymous or pseudonymous credentialing systems. While some sections do point to anonymous and pseudonymous credentialing systems as an option, even in those cases it appears to assume some sort of individualized full authentication, at least to the CSP (see, for example, lines 668-671 of SP-800-63-4). The implication is that at least one party in the complex multi-party system needs to have a unique identifier for the user, even in scenarios where unique identification explicitly isn't necessary. This default assumption limits the privacy gains that are possible with more advanced architectures (such as the IETF's PrivacyPass credentialing) in those scenarios where full unique, re-linkable identification isn't necessary. For an example of a digital credentialing system that takes these concerns seriously, see Wang et al, Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution, 2023, in which the authors build a system in collaboration with the Red Cross to authorize refugees to receive benefits, without creating an identity database that could become a means of abuse of vulnerable and persecuted refugee populations. Given the expanded attention to digital wallets which offer more support for these mechanisms than solutions that actively involve an IdP in each presentation, SP-800-63-4 should include more substantive discussion of and pointers to pseudonymous or, preferably, anonymous authorization mechanisms, and how they can be deployed to authorize access to government systems.

V. NIST Should Rethink Its Approach to User Groups

NIST wants agencies to evaluate the impact of digital credentialing on user groups, but it defines user groups by their privileges in the system rather than by their real-world identities (P-800-63-4, lines 1017-1020). This is a common breakdown used by designers of technical systems, but the specific technical role assigned to the user is hardly the most relevant way to categorize them. For example, a resident applying for state assistance related to temporary physical disability might use the same technical role in a benefits system ("applicant") as someone at risk of or fleeing domestic abuse. But despite their "user group" being the same, their specific concerns (related to identity proof, privacy, family transparency, etc.) might be entirely different. When people with different needs are lumped together, the more marginalized subgroups typically lose out. Because assurance levels must work for everyone, the most encumbered subgroup should set the baseline standard for the online service. A more nuanced breakdown of different categories of affected

people (users or not) might uncover distinct risks or failure modes that need different forms of mitigation. When conducting more nuanced research into user groups, agencies should work with their SAOPs to ensure privacy best practices are employed to ensure marginalized subgroups do not have additional PII collected and stored about them which may create new privacy and equity risks.

CONCLUSION

The ACLU and EPIC welcome NIST's leadership on digital identity standards, which come at a crucial time for government agencies seeking to modernize their systems and implement more sophisticated forms of identity verification.

We appreciate this opportunity to reply to NIST's Request for Comment and are willing to engage with NIST further on any of the issues raised within our comment. For any further questions, please contact ACLU Senior Staff Attorney Olga Akselrod [redacted]), ACLU Senior Technologist Daniel Kahn Gillmor [redacted], EPIC Counsel Grant Fergusson [redacted], or EPIC Counsel Suzanne Bernstein [redacted]

Respectfully submitted,

/s/ Daniel Kahn Gillmor
Daniel Kahn Gillmor
ACLU Senior Technologist

/s/ Grant Fergusson
Grant Fergusson
EPIC Counsel

/s/ Olga Akselrod
Olga Akselrod
ACLU Senior Staff Attorney

/s/ Suzanne Bernstein
Suzanne Bernstein
EPIC Counsel