April 14, 2023

National Institute for Standards and Technology
100 Bureau Drive (Mail Stop 8940)
Gaithersburg, Maryland 20899-2000

Re: Digital Identity Guidelines

To: David Temoshok et al.

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the National Institute for Standards and Technology's (NIST) call for comments on its draft of version four of the Digital Identity Guidelines (Special Publication 800-63).[1] CDT is pleased to see that NIST has taken steps to account for equity and privacy in the identity management process in this draft. CDT provides the following comments in order to advance these goals and ensure that they are effectively implemented. CDT believes that by making these changes, NIST will be better able to help government agencies and other organizations serve customers effectively and equitably while protecting their privacy and guarding against irresponsible practices.

CDT's feedback is organized into two sections:

- Global comments that apply across volumes or to multiple volumes, and
- Volume-specific comments that apply to specific aspects of the four volumes that comprise the digital identity guidelines

Global Comments

Alternatives to the use of biometrics for identity proofing and verification

Meaningful certification that accounts for equity concerns

One set of particularly positive changes relates to the levels of certification for identity proofing that NIST puts forward. First, CDT is happy to see that NIST recommends that organizations implement a wide variety of identity validation and verification techniques in order to help users with differing levels of technological access.[2] Not all users have the same access to technologies or identity documents that different identity proofing methods require. Second, the

[1] NIST, SP 800-63-4 (Draft) Digital Identity Guidelines, (Dec. 16, 2022), https://csrc.nist.gov/publications/detail/sp/800-63/4/draft#pubs-documentation.
[2] Volume A, Page 6, Section 4. Identity Resolution, Validation, and Verification, Lines 438-444

updates to both IAL1 and IAL2 are helpful.[3] Both contribute to creating a standard for meaningful guarantees on identity proofing without requiring the use of biometrics, which was practically unachievable under the previous guidance. These updates will allow companies and other entities to have a level of confidence in their identity proofing frameworks without requiring overly-invasive data collection.

Suggested Changes

Provide further guidance about deciding which certification level is appropriate
While not a direct change to the identity management guidance, NIST should further promote and encourage the use of IAL1 as a valid certification level. Wider adoption of IAL1 would ultimately mean more applications that are less onerous and privacy invasive for users and that still provide a clear standard of identity management for applications that do not need the level of confidence provided by IAL2 and IAL3. To encourage adoption of IAL1, NIST could offer webinars or other guidance about how to implement IAL1 systems and the benefits it provides over a non-compliant approach. Furthermore, NIST should provide examples of applications that are appropriate at each of the IALs.[4] One way that NIST would know if this work is succeeding is if identity management vendors began to feature products that come with IAL1 certification in addition to products that carry IAL2 certification.

Encourage increased transparency and community engagement
To help organizations assess the possible consequences of choosing between different IALs, NIST helpfully provides a framework for organizations to make this decision.[5] However, while the suggestions about which types of impact to consider are good, NIST does not require that organizations consult communities and end-users about potential impacts. Instead, NIST only requires that organizations assess potential risks without further clarification, leaving it up to organizations to determine how to perform risk assessment. Community engagement is an essential part of this risk assessment, as members of the impacted community will have unique insights into how they expect to use the system and the risks of a failure in the system.[6] These insights will be critical to ensuring that the risks to the community are appropriately addressed.

Alternative evidence other than biometrics for IAL2

This edition clarifies the verification requirements for IAL2, allowing for either biometric comparison or possession of a digital account to count as evidence.[7] This clarification will

[3] Volume A, Pages 26-27, Section 5.3 Identity Assurance Level 1
[4] Base Volume, Pages 32-33, Section 5.2.3.1. Selecting Initial IAL
[5] Base Volume, Pages 29, Section 5.1.4. Impact Analysis
[6] Elizabeth Laird & Hugh Grant-Chapman, *Report – Sharing Student Data Across Public Sectors: Importance of Community Engagement to Support Responsible and Equitable Use*, CDT, Dec. 2, 2021. https://cdt.org/insights/report-sharing-student-data-across-public-sectors-importance-of-community-engagement-to-support-responsible-and-equitable-use/.
Washington State Department of Health, *Community Engagement Guide*, Accessed Mar. 17, 2023. https://doh.wa.gov/sites/default/files/legacy/Documents/1000/CommEngageGuide.pdf.
[7] Volume A, Page 33, Table 1. IAL Requirements Summary

hopefully allow more organizations to verify identities without the use of biometrics. This is a welcome change because, while biometric systems can provide some benefits and functionality, they also raise important equity concerns. Biometric comparison systems can perform variably across different populations in ways that introduce or perpetuate inequities.[8] Additionally, these systems may require a level of technological access or sophistication that not all of the target population possess.[9]

To further strengthen alternative verification methods that are compliant with IAL2, NIST should make the requirements for possession of a digital account more robust. The first mention of control of a digital account as a method of identity verification alludes to "the use of authentication or federation protocols."[10] Further detail is provided in Volume A, Section 5, which explains that the user must have, "Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation protocol."[11]

However, merely possessing a digital account with AAL2 authentication and FAL2 federation standards may not be enough to prove identity. AAL2 authentication helps assure that only the user who initially created the account is now accessing the account, while FAL2 federation helps assure that information is shared securely between the identity provider of the digital account and the relying party.

Fraudsters can create fake bank accounts or mobile driver's licenses using other people's information. It seems implicit that NIST is relying on the third party providing the digital account (such as the bank) to have performed some identity proofing themselves. However, the identity proofing performed by the third party needs to have been at least as strong as IAL2. Otherwise, a fraudster could create a fraudulent account at an organization using only IAL1 or weaker standards, and then use that digital account to pass IAL2 proofing elsewhere.

Suggested Changes

Add requirement to identity proofing re: digital account possession
In Volume A, NIST should be clearer and more explicit about the identity proofing requirements for a digital account that is intended to be used in future identity proofing at the IAL2 level.

Add additional alternatives to biometrics and digital account possession
Additionally, NIST should consider other alternatives to biometrics, including approaches like verification via physical address and data sharing with known partners like other federal or state

[8] Jacqueline Miller, Mary Lou Breslin, & Susan Chapman, *Impact of Electronic Visit Verification (EVV) on Personal Care Services Workers and Consumers in the United States*, San Francisco, CA: UCSF Health Workforce Research Center on Long-Term Care, July 22, 2021. https://dredf.org/wp-content/uploads/2021/08/EVV-Report-210722.pdf.
[9] Andrew Kenney, *System for unemployment benefits exposes digital divide*, AP News, May 2, 2021. https://apnews.com/article/digital-divide-technology-business-health-coronavirus-429ca0ef19108f2a6c99c4d812abe10b.
[10] Volume A, Page 15, Section 4.4.1. Identity Verification Methods, Lines 684-688
[11] Volume A, Page 29, Section 5.4.4.1 Remote Identity Proofing, Lines 1133-1144

agencies. These approaches carry different risks and benefits from biometrics, and so may be more appropriate in some contexts. For instance, verification via physical address (such as sending a piece of mail with an activation code to a known address) may be too slow or onerous for some applications, but it may be more accessible than a biometric login for users who do not have smartphones.[12]

More detailed guidance on appropriate use of biometrics

Some organizations inevitably will choose to use biometrics for identity verification. When this is the case, the additional requirements on efficacy, equity, and privacy in this version of identity management guidance are critical.[13] However, NIST should include some additional requirements to ensure that the equity and privacy risks of incorporating biometrics are appropriately weighed against the confidence benefits.

Suggested Changes

Provide clear guidance on data governance requirements for biometric data
Because of the sensitivity and irrevocability of biometric data, it is critical that those collecting such data implement strong data governance frameworks to manage it. NIST should provide guidance about key elements of these frameworks. This guidance should include prohibitions or limits on its use for secondary purposes, sale or transfer to third parties, and retention. Additionally, processors of biometric information should follow security best practices, such as encrypting biometric data and preventing unauthorized access to said data, including among internal employees.

Provide additional flexibility on performance thresholds
Furthermore, NIST stipulates performance thresholds that biometric technologies should meet.[14] In particular, NIST requires that only 1 out of 10K attempts results in a false match and only one 1 out of 100 attempts results in a false non-match. These thresholds encode the idea that false matches are costlier than false non-matches, presumably because individuals who receive false non-matches would ideally have other recourse. On the other hand, a false match may lead to a case of fraud which is difficult to discover and correct.

While these thresholds are a helpful starting point, NIST should also clarify that that organizations may choose to enforce different standards above the minimum that capture different trade-offs between false matches and false non-matches, particularly as there are already vendors that are able to offer products that can meet more stringent standards.[15]

---

[12] Michael Yang, *Digital Identity Verification: Best Practices for Public Agencies*, CDT, Oct. 24, 2022. https://cdt.org/insights/digital-identity-verification-best-practices-for-public-agencies/.
[13] Volume A, Page 22, Section 5.1.8. Requirements for Use of Biometrics, Lines 917-958
[14] Page 23, Lines 935-937
[15] NIST, *Face Recognition Vendor Test*, Accessed Mar. 17, 2023. https://pages.nist.gov/frvt/html/frvt11.html.

Equity and Accessibility

CDT is pleased to see that NIST has incorporated equity considerations so heavily into this iteration of the guidance. The examples in lines 2455-2468 are useful in illustrating the types of equity challenges faced by different users, including disabled users. However, this is somewhat at odds with the statement at line 2093 that accessibility is out of scope for this document (and the corresponding statements at lines 1495 of Volume A and 1888 of Volume C), as accessibility is a critical component of equity.

Suggested Changes

Clarify accessibility guidance
NIST should make clear that the *how* of accessibility may be out of scope for this document (and provide helpful pointers as they do at line 2538), but that the fact of accessibility is a critical component of an authentication system. Though the federal government may be beholden to specific requirements, private companies may require more specific guidance and clarity about the risks of failing to build an accessible system.

Volume-Specific Comments

Base Volume

Section 2.3.3
CDT commends NIST for specifically recognizing the underserved nature of disabled people, as this is a group that has been frequently under-considered in the building of technical systems, even when they may need to make proportionally more use of those systems than non-disabled people.

CDT recommends re-ordering paragraphs 3 and 4 of this section to make clear that federal agencies are directed to do this work, rather than presenting it as something more optional. For non-federal agency organizations, CDT recommends strengthening the language in paragraph 3 from “encouraged” to something more forceful such as “strongly encouraged” or “NIST recommends that…”.

Sec. 2.3.4
CDT commends NIST for explicitly calling out usability as a consideration. CDT also recommends that they note that usability is also an important avenue for enhancing equity and efficacy. Usable systems that work for everyone are also more accessible to users less familiar with technology, which can intersect with other avenues of discrimination.[16] Additionally, users

[16] Andrew Kenney, *System for unemployment benefits exposes digital divide*, AP News, May 2, 2021. https://apnews.com/article/digital-divide-technology-business-health-coronavirus-429ca0ef19108f2a6c99c4d812abe10b.

are less likely to search for potentially insecure workarounds (thus subverting developer expectations) when they are interacting with a usable system, ultimately making the system more secure and effective.

Volume A

Sec. 5.1.3
CDT appreciates the guidance to Credential Service Providers (CSPs) to document equity mitigations they make. In addition, CSPs should also document sources of risk of inequitable access, treatment, or outcomes that they have identified as part of their risk assessment process.

Volume C

Sec. 9.2
CDT appreciates that the guidance provides information about what makes for meaningful notice to ensure that users are adequately informed about how the system will use their data. The guidance could provide more information about the consent component, namely, how to solicit meaningful consent, and how to be clear with users about what will happen in the event that they do not provide consent.

We appreciate the opportunity to submit these comments. NIST's ongoing commitment to equity is commendable, and we hope that this input will help to further that goal.

Sincerely,
Elizabeth Laird
Director, Equity and Civic Technology Project, CDT

Hannah Quay-de la Vallee
Senior Technologist, CDT

Algorithmic Justice League

Milda Aksamitauskas
Fellow, Beeck Center for Social Impact + Innovation at Georgetown University

Elizabeth Bynum Sorrell
Project Researcher, Beeck Center for Social Impact + Innovation at Georgetown University

Ariel Kennan
Fellow, Beeck Center for Social Impact + Innovation at Georgetown University

Aaron Snow
Fellow, Beeck Center for Social Impact + Innovation at Georgetown University