CENTER FOR
DEMOCRACY
& TECHNOLOGY

October 7, 2024

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

Re: Digital Identity Guidelines - Revision 4 - 2nd Public Draft

To: David Temoshok et al.

The Center for Democracy & Technology (CDT) respectfully submits this comment in response to the National Institute of Standards and Technology's (NIST) call for comments on the second public draft of revision four of the Digital Identity Guidelines (Special Publication 800-63).

CDT is pleased to see that NIST has taken steps to account for equity, access, and privacy in the identity management process in this draft. CDT provides the following comments in order to advance these goals, particularly in the context of public benefits administration, an area where providing customer-centered, privacy-forward, multi-modal identity verification is paramount for protecting vulnerable individuals and people experiencing hardships while streamlining their access to life-saving benefits.

Global Comments

CDT commends NIST for the myriad changes to its digital management guidance that advance privacy, access, and equity. It is critical that NIST not only maintain these advances but continue to center these values. In particular, CDT is heartened to observe the following changes that help public agencies better meet the needs of public beneficiaries:

- Equity and accessibility have been explicitly incorporated throughout the guidance, giving agencies clear avenues to consider the diverse and complex needs of populations they serve.
- NIST has emphasized the need for optionality, particularly across different modalities and formats (including analog and in-person options). These varied avenues help to ensure that users are not excluded from critical services due to limited technology access.

Volume-Specific Comments

Base Volume

3 - Digital Identity Risk Management

We appreciate that the structure of the Digital Identity Risk Management (DIRM) process provides flexibility for relying parties (RPs) to ensure that their identity system addresses the specific needs of their user population. As noted above, this is particularly critical for public benefits systems, whose users are disproportionately likely to face barriers in proving their identity due to factors that range from lack of access to traditional identity evidence to limited technology access or mobility. Addressing these barriers may add complexity to the process of building an identity management system, but it is a critical improvement for ensuring that the systems are equitable and accessible.

Suggested Change

Emphasize documentation as part of the iterative DIRM process
We appreciate that the process of assessing the system described in Figure 6 explicitly highlights that the DIRM is an interactive process, a key component of which is appropriate documentation. Consequently, Step 5 of Figure 6 should include "documentation" as part of the "Implement/Deploy/Adjust" cycle. This will help to ensure that knowledge about the system, any adjustments made to it, and the reasoning and intention behind those adjustments are accessible throughout the lifecycle of the system.

3.1 - Defining the Online Service

As mentioned above, we commend NIST for incorporating a focus on equity, access, and privacy. We appreciate that NIST has threaded these considerations through the guidance in a number of ways, and recommend additional places where these values should be incorporated.

Suggested Changes

Consider access to identity evidence for specific populations
We appreciate lines 1090-1091, which require RPs to assess the availability of identity evidence for the populations they serve. NIST should add that RPs should not only consider this as a whole, but also for specific sub-populations of their user group. For instance, it may be the case that, in general, most of their users possess necessary identity evidence, but the population that does not is disproportionately elderly. In such a case, the potential for failure would not be borne equally by the user population, and the RP may need to take specific steps to ensure their systems do not disproportionately impact certain populations, particularly those who have been historically marginalized. (This more granular demographic analysis is suggested by lines 567-570: "To support the continuous evaluation and improvement program described in Sec. 3, it is important to maintain awareness of existing inequities faced by served populations and potential

new inequities or disparities between populations that could be caused or exacerbated by the design or operation of digital identity systems," but should be made explicit in the discussion of defining the online service, particularly as lines 567-570 are informative, rather than normative.)

Provide in-person proofing options if the user population requires it
In addition to assessing the availability of evidence for users served, RPs should also assess their intended users' ability to participate in different forms of proofing, in particular whether some of their users may require an in-person proofing option in order to complete the proofing process. If some of their users will require access to in-person proofing in order to complete the process (whether because of lack of technology access or discomfort or inability to use technology), the RP should be required to provide an in-person option. (This change is not necessary if, as suggested below, Volume A is adjusted to require an in-person avenue as part of the optionality requirements for identity proofing.)

Use the same scenario to describe "user groups" and "impacted entities"
The distinction between users and impacted entities is helpful, and we appreciate the explicit inclusion of broader societal impacts of identity systems and the systems they aim to protect. The explanation of the difference between the two in lines 1104-1115 would be clearer if both examples were drawn from the same system of framework. So, rather than using an income tax system and a water treatment facility, select one system example that includes both user groups and impacted entities. One potential example could be something like dedicated apartments for unhoused individuals in a larger building, where the tenants of the dedicated apartments would be the users, while the impacted community would be the residents of other units in the building.

3.4 - Tailor and Document Assurance Levels

As discussed, we commend NIST for establishing a risk management approach that allows organizations to account for the specific needs of their population. We appreciate that lines 1507-1512 specifically direct organizations to consider the impact of their identity management system on marginalized and underserved populations and to consider both outcomes like failure rates but also process considerations like friction. We also appreciate NIST's specific inclusion of equity in the assessment process.

Suggested Changes

Incorporate "mission delivery" into the tailoring process
To ensure that organizations account for all the relevant factors in their tailoring process, NIST should add "mission delivery" to "specific context, users, and threat environment" in lines 1505-1506. This will underscore the need to maintain their ability to achieve core objectives when assessing their identity system.

Consider all factors in equity assessments, including gender identity
In lines 1567-1571, NIST should add gender identity to the list of factors for organizations to consider.

Document risks of compensating controls
In lines 1622-1624, organizations are required to document their compensating controls and other relevant information. Organizations should *also* document any new risks, whether to the system being protected by the identity system or any other parties, particularly users, introduced by the new control. (For instance, in the example in lines 1618, stricter auditing controls may increase the likelihood of blocked transactions, which may be a reasonable trade-off with respect to other factors, but should be documented.)

Use proofing types as compensating controls, or adjust evidence strength for in-person proofing
In the context of identity proofing, an additional avenue of tailoring that NIST should consider incorporating is that of adjusting evidence strength for different proofing types. IAL1 is designed to address scalable attacks, and IAL2 is designed to limit scalable and targeted, but not sophisticated, attacks; in-person proofing serves as a significant barrier to scalability and a disincentive for targeted attacks, particularly if the proofing occurs in an environment like a government office where significant surveillance is likely to occur. Due to this, NIST should consider allowing for in-person proofing to serve as a compensating control that allows for the acceptance of weaker evidence for IAL1 and potentially IAL2 in contexts where doing so would increase the accessibility of proofing for individuals and populations with limited access to identity evidence, particularly evidence in the STRONG category, as the exemplars of STRONG evidence consist of government-issued IDs, which can be an access limitation for some historically marginalized populations.

Volume A

2.5 - Identity Verification

Lines 799-808 describe a visual facial image comparison conducted by a human. It notes that, if the comparison is performed at a later time, rather than live, steps should be taken to ensure that the image or video was captured live. NIST should add that even in a live comparison context, verifying organizations should do what they can to ensure the image or video is authentic. This is particularly important as generative AI systems become more sophisticated and able to impersonate individuals with relatively little reference data.

3.1 - General Requirements

CDT appreciates that NIST has provided numerous requirements governing the use of biometric systems, as biometrics are an incredibly sensitive method of verification. NIST should maintain these requirements in the final guidance to ensure that users of identity verification systems can expect and experience equitable treatment.

Suggested Change

Include disability and gender identity when evaluating biometric performance
To further enhance the equity of these systems, NIST should add disability and gender identity to the list of demographic groups in line 1262. These are two populations where there is a

dearth of evidence for how biometric comparisons, particularly facial recognition systems, perform when trying to identify individuals. Consequently, NIST should emphasize the need for organizations to ensure that these populations are not disproportionately failed by biometric identity management systems.

3.1.8 - Requirements for Confirmation Codes

CDT commends NIST for including validated physical addresses as an option for confirming confirmation codes, alongside telephone numbers and email addresses in lines 1147-1148. This is an important inclusion for populations who lack consistent or comfortable access to technology. We urge NIST to maintain this avenue for verification in the final guidance. Additionally, we appreciate that NIST identifies maximum validity times for codes (21 and 30 days when sent to validated domestic and international postal addresses respectively) that allow sufficient time for codes to reach users (lines 1157-1160). NIST may wish to consider recommending minimum time periods for codes to remain valid in addition to the maximum validity periods, to balance avoiding codes expiring too quickly for users to be able to receive and use them with creating potential security risks. (For further discussion of expiration of physical codes, see comments filed by the Digital Benefits Network, Beeck Center for Social Impact + Innovation at Georgetown University.)

4 - Identity Proofing Requirements

The delineation of different types of proofing is valuable, as different proofing types carry different risks and benefits. NIST should require or encourage organizations to offer the widest variety of services necessary to serve their user populations.

Suggested Change

Require an in-person proofing option
The incorporation of the need for different options of identity proofing to serve different users is beneficial and will help to ensure that organizations can meet the needs of diverse populations. However, NIST should include a requirement for an in-person proofing mechanism, attended or unattended, in IAL1 (lines 1505-1516) and IAL2 (lines 1655-1665), unless the organization is able to ensure that all of their users will be able to complete an online proofing process without difficulty. In-person proofing can be critical for individuals with limited technology access or comfort, which in some contexts, including public benefits delivery, is a disproportionately large percentage of the population an organization is intended to serve. (For further discussion of the need for in-person proofing avenues, see comments filed by the ACLU.)

4.4 - Summary of Requirements

CDT appreciates that NIST has expanded IAL1 into a viable identity proofing tier, rather than an absence of proofing. This is critical in that it provides a meaningful level of proofing that does not require a state issued identification or a biometric comparison. This is essential for the establishment of equitable and accessible identity systems, and NIST should ensure that this is retained in the final guidance.

7.4 - Redress

Redress mechanisms are incredibly important in ensuring that identity systems function as needed and provide access to all legitimate users, including those who may fall into edge cases, so we commend NIST in incorporating this element and stressing the usability and accessibility requirements.

Suggested Change

Consider informing applicants of causes of failure in some cases
In line 2124, the guidance notes that credential service providers (CSPs) should not inform the applicant of the specific reasons that their registration failed. While this is very reasonable in most cases, and is important for protecting the integrity of the system, there are some cases where this could present a barrier to usability without specific security gain. In particular, if the failure is due to missing information, not providing that information to an applicant may be a significant barrier to their ability to remedy the absence and complete the verification process. NIST should consider whether there are specific failure cases where CSPs should communicate the issue to applicants.

Volume C

5 - Subscriber-Controlled Wallets

CDT appreciates the inclusion of subscriber-controlled wallets, as it enables organizations to use modern identity management techniques while adhering to the ID Digital Management Guidelines. Maintaining subscriber-controlled wallets allows for users to maintain control of their identity documents and retain agency in when and how their information is used, so we appreciate NIST understanding the valuable role they play in the identity ecosystem, a role that is likely to grow significantly over time. Nevertheless, subscriber-controlled wallets can only provide comprehensible and acceptable privacy protections for users if they fully satisfy requirements for genuine user control, unlinkability, selective disclosure, informed consent and accountability. The Digital Identity Guidelines provide an opportunity to describe how a federated identity system – including issuers, relying parties, and wallet software providers – can satisfy all these conditions.

Suggested Changes

Enable user choice in selection of wallet providers
To ensure the user-agency aspects of a subscriber-controlled wallet are maintained, security measures must enable user control. So while ensuring baseline security measures are implemented in order for a subscriber-controlled wallet to be a valid form of identity evidence, NIST should ensure that in the final version of the guidance those security measures do not amount to locking users into a wallet that may not act on their behalf or acts in ways the user does not intend.

Require user control of individual wallet attributes
Additionally, users should maintain control of the attributes of their wallet. Currently this is an optional trait of wallets; lines 2631-2632 state that “The subscriber-controlled wallet SHOULD provide a means to selectively disclose a subset of the attributes in the attribute bundle from the CSP.” Changing the SHOULD to SHALL would increase user agency over their own information.

7 - Privacy Considerations

We appreciate NIST drawing attention to the privacy considerations that can arise from a federated approach. However, the fact that the Privacy Considerations section is informative, rather than normative, means that users are not guaranteed critical privacy protections.

Suggested Changes

Require key privacy considerations to be incorporated
NIST should consider making the Privacy Considerations section normative and assigning some key privacy protections “shall-do” status. In particular:

- Presentations of an ID from a mobile wallet must be unlinkable across different organizations.
- Issuers should be grouped in such a way that presenting a single claim does not reveal the institution that issued a particular credential.
- Technical protections against collusion for tracking must be required, not just recommended.

Expand notice and consent provisions
Informed consent requires in-context explanation of the purpose, justification, and limitations under which user identity information is disclosed. That must include not just which attributes are accessed by which relying party, but also why data is being requested, how data will be used, and whether data will be retained or shared. The current section on Notice and Consent does not provide these necessary conditions. In addition, the expectation that some data will be shared automatically based on an allowlist without the user’s participation is not consistent with consent.

Establish reporting frameworks for inappropriate collection or use of wallet information
Accountability requires a way to meaningfully report abuse – like asking for information inappropriately – and a system to investigate, evaluate, and address that abuse. While abuse handling is a governance function, technical design and requirements can support it. For example, use cases should be registered with a relevant data protection authority and documented in a machine-readable way for consumption by subscriber-controlled wallet software. Wallet software should provide abuse reporting functionality.

We appreciate the opportunity to submit these comments, and appreciate the significant work that NIST has done to incorporate privacy, equity, and usability into the guidance. The changes already made to the guidance are a significant step forward in helping to build identity management systems that serve people, and we hope that these comments can help NIST continue to push towards that end.

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

Hannah Quay-de la Vallee
Senior Technologist, CDT

Nick Doty
Senior Technologist, CDT