Comments to NIST

SP 800-63-4 Digital Identity Guidelines (Draft)

April 2023

The Better Identity Coalition appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on its draft fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 23 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In July of 2018, we published *Better Identity in America: A Blueprint for Policymakers*[1] – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S. Privacy is a significant focus: the Blueprint detailed new policies and initiatives that can help both government and industry deliver next-generation identity solutions that are not only more secure, but also better for privacy and customer experiences.

We note that we are encouraged to see NIST launching this new revision of SP 800-63-3. While the 2017 publication of SP 800-63-3 represented a significant improvement in NIST's Digital Identity Guidelines, technology and threat are never static. We believe there are a number of places where industry and government alike will benefit from a refresh of Guidance that reflects changes over the last few years. We are encouraged to see that NIST is embarking on another revision of the document.

Up front, we note that we were pleased to see that many of the issues we raised in our August 2020 comments to NIST (in response to NIST's pre-draft call for comments) were addressed in the new draft. We understand that NIST faces a notable challenge in trying to address inputs from dozens of different stakeholders, and appreciate NIST's willingness to consider our inputs.

We are submitting comments regarding specific sections and wording in the formal Excel comment template you published.

Additionally, we have a number of higher level comments that respond to some of the questions NIST asked in its December 16th announcement. Those follow below.

Note that NIST's questions are italicized; our responses are not:

[1] See https://www.betteridentity.org/s/Better_Identity_Coalition-Blueprint-July-2018.pdf

Identity Proofing and Enrollment

- *NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provides security and convenience, but does not require face recognition. Accordingly, NIST seeks input on the following questions:*
    - *What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?*
    - *Are these technologies supported by existing or emerging technical standards?*
    - *Do these technologies have established metrics and testing methodologies to allow for assessment of performance and understanding of impacts across user populations (e.g., bias in artificial intelligence)?*

  A number of our members believe there are ways to conduct unattended, fully remote identity proofing without biometrics in a way that achieves performance (in terms of real identities approved, real identities rejected, false identities mistakenly approved, and false ones caught) that is commensurate with what IAL2-certified solutions deliver today – though we note that not all of our members agree on this point.

  The challenge with these sorts of alternative solutions is that they tend to rely on approaches that, while innovative, are proprietary and are not supported by standards. For NIST – an agency devoted to measurement science – it is thus a challenge to measure their effectiveness.

  That said, it should be theoretically feasible to measure effectiveness of alternative approaches to remote identity proofing by conducting testing of IAL2-certified solutions – to establish a benchmark as to what those products can deliver today – and then conduct testing of alternative solutions to see if they can meet those same performance metrics. If so – then it could be reasonable to redefine IAL2 to focus less on process and more on outcomes. This is a topic where a number of our members have additional, specific ideas that may be worth exploring.

- *What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?*

  At the moment, both mDLs and VCs are new, emerging standards; work is still ongoing around both efforts. In mDLs, for example, the ISO 18013-7 standard focuses on remote identity proofing, but work on that standard is not yet complete. There are not yet widely adopted standardized ways to use mDLs and VCs in remote identity proofing. We were encouraged to see NIST's NCCoE launch a new initiative in March focused on this effort – we believe NIST's leadership on this issue will be critical to enabling new ways to enable remote identity proofing that are easier and more equitable for users.

With regard to mDLs and VCs, some of our members have noted that while they are powerful new tools, implementers will still want to augment them with the use of real-time identity resolution and risk mitigation methods including synthetic and identity fraud checks, plus the use of device-based fraud checks.

Additionally, SP 800-63A should allow mDLs to be used in an identity proofing process without the user being required to re-enroll their physical credential. It is also important that the guidelines give credence to the verification at source of the biometric and biographic data in assessment of strength. This means both that a poorly issued digital credential isn't given greater weighting than its physical counterpart and that the strength of a robustly issued digital credential is carried through to the identity proofing process.

- *What are the impacts, benefits, and risks of specifying a set of requirements for CSPs to establish and maintain fraud detection, response, and notification capabilities?*
    - *Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?*
    - *How might emerging methods such as fraud analytics and risk scoring be further researched, standardized, measured, and integrated into the guidance in the future?*
    - *What accompanying privacy and equity considerations should be addressed alongside these methods?*

      Fraud checks like the ones described in this question are becoming increasingly important – however a number of our members have noted that if NIST is overly specific in the tools that should be used, it may inadvertently lock implementers into a compliance-based approach that focuses more on "checking the box" on specific controls and less on taking a true risk-based approach; the latter allows fraud checks to evolve with time as both threat and technology evolve. For this reason, it may be best to avoid calling specific controls out as normative requirements. Otherwise, as technology and threat changes, prior fraud checks may be replaced with new ones making conformance difficult on CSP's going forward.

      This is because industry provides risk insights differently across vendors, making specificity difficult to document within guidance, except, perhaps, at the highest assurance level.

      That being said, guidance that references known and accepted high level fraud checks as examples of the types of tools that might be used can be referenced within guidance to provide underlying support for CSP assessment processes who chose to use them as risk mitigations for choices that are appropriate to them.

Authentication and Life Cycle Management

- *Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks?*

  Passkeys seem to be properly addressed in the new guidance – though more guidance on how to secure the "sync fabric" associated with multi-device passkeys could be helpful.

  VC and mDL – as noted above – are still evolving. The fact that this draft references them as being able to be used in identity proofing is helpful, as it recognizes their utility and also helps to "future proof" this document. However, we expect that NIST may need to create supplemental guidance at some point to account for just how VCs and mDLs may be used, and/or update this next revision with additional language. It is also not clear, however, that they will have a role to play as authenticators; we see their primary value in the identity proofing sphere.

- *Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?*

  We believe these look solid. However, it would be good to note what standards (x.509, FIDO, etc.) can be used to address the two approaches to phishing resistance in the body of the document, to make this clear to implementers.

General

- *Is there an element of this guidance that you think is missing or could be expanded?*

  One of our members suggested that it would help to increase equity and access across diverse populations by clarifying and expanding that Remote Supervised proofing can also be used at IAL 1 and IAL 2 vs specifically referencing at only IAL 3.

  A second suggestion is that NIST look to build in accommodations for the safe use of "pay-as-you-go" mobile phones given their prominence with some demographics. Finding ways to support those devices within omni-channel identity services could provide support to CSPs in the use of such devices which is supportive of equity and inclusion.

- *Is any language in the guidance confusing or hard to understand? Should we add definitions or additional context to any language?*

  In general, we believe NIST should look to incorporate key elements of its Implementation Resources into the main body of the four documents. Right now these Resources are published as a standalone document, and for all practical purposes, many implementers do

not even know they exist, or if they do, may find it cumbersome and/or exhausting to match up elements of the Implementation Resources with the content in the main body of the document.

In other words – wherever practicable – ensure that someone can get their questions answered from one document rather than requiring them to review two.

- *What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?*

  One challenge facing agencies and other implementers is that neither they nor industry have a standardized set of metrics or common language by which to assess performance of different solutions and articulate impact on their user bases. For example, today third-party organizations assess whether a CSP is compliant with SP 800-63 requirements, but four CSPs that are all compliant with IAL2 (as one example), may deliver wildly varying performance when used in real world applications. With an increased focus on assessing not only how well a solution performs but also whether it performs differently across different demographic groups, additional work is needed.

  As a starting point, NIST should work with industry to define a set of common metrics that accreditation bodies or other organizations such as third-party labs can use to validate performance of CSP's. This will promote trust and confidence among agencies and other implementers.

  With this, NIST could consider working with industry to define user populations that could factor into performance testing. For example, testing could explore if and how different providers handle international users, tribal users, users with housing insecurity challenges, users that have had a recent name change, those that do not speak English, or those that may require assistive technology like screen readers.

  As NIST and DHS do with facial recognition test results, performance data that has been validated or established by independent third parties could be made public. This sort of standardized and transparent performance metrics will allow comparison of providers relative to each other.

We greatly appreciate your willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at jeremy.grant@venable.com.