Comments to NIST

Pre-Draft Call for Comments: Digital Identity Guidelines

August 2020

The Better Identity Coalition appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on its Pre-Draft Call for Comments: 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 – 22 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.

Up front, 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.

We have divided our comments into three categories, aligning with the three parts of SP 800-63-3.

1. Enrollment and Identity Proofing

- *Consider additional capabilities that would allow remote identity proofing solutions to achieve equivalent IAL as in person proofing.* The importance of robust remote identity proofing solutions has only increased amidst the COVID-19 pandemic, and organizations are struggling to find ways to conduct high assurance identity proofing without requiring an in-person appearance. NIST would do the country a great service in assessing the range of solutions in market today and outlining additional ways that organizations can conduct high assurance, remote identity proofing.

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

One of our members has suggested that NIST should explore if there are mechanisms to support asynchronous video-based verification, where the video is authenticated after it has been captured.

- *To the point above, consider referencing new government attribute validation services such as eCBSV or DLDV as an alternative to physical document checks.* Paper documents are easily forged and do not offer significant security value. As new government digital attribute validation services launch, it would be helpful for NIST to point implementers to those alternatives.

- *Consider providing performance metrics for selfie-to-credential face matching.* The use of these tools has exploded in the market since NIST guidance was last updated in 2017. Groups including FIDO Alliance have launched new programs to develop performance requirements and certification programs for these new remote ID verification tools. It may be helpful for NIST to provide guidance as to the acceptable FAR/FRR of biometric matching in these tools.

- *Consider explicitly stating that REAL ID compliant identification documents satisfy the IAL2 "One piece of STRONG evidence" requirement*, if they have been validated at an authoritative source. Currently, a REAL ID conformant proofing process may allow an applicant to present a single piece of SUPERIOR or STRONG evidence if that piece of evidence satisfies two qualification categories. Unless a CSP has extensive access to the DMV proofing records, the CSP will not know if one or two pieces of evidence were evaluated by the issuing DMV.

- *Explore ways to leverage new tools to make IAL2 compliance easier.* A key driver behind the founding of the Better Identity Coalition was to address the need for next-generation remote identity proofing solutions. As we have pointed out in our Policy Blueprint, attackers have caught up with many legacy tools used in remote identity proofing; we have outlined our belief that the government needs to play a role to help drive new solutions here.

  While much of this government work goes beyond anything that NIST alone can do, there is a notable gap between the number of applications that require IAL2 identity proofing and the practicality of implementing an IAL2 solution. As NIST has no doubt heard from many parties, IAL2 has been quite difficult to implement in practice – the bar for achieving IAL2 has been set quite high. While the security requirements around IAL2 are rightfully robust, there is a need to balance security against practicality. To the extent that NIST can explore whether the current requirements for IAL2 are fully necessary to meet the risks involved with IAL2 applications – and adjust accordingly – it will be helpful in making IAL2 something that is not just a theoretical notion to strive for but a standard that is easily realized.

2. Authentication and Lifecycle Management

- *Increased recognition of dynamic, risk-based authentication solutions.* Perhaps the biggest critique our members have flagged with regard to SP 800-63B is that it lays out an authentication model that is disconnected from the way many organizations actually implement authentication. It is rare for enterprises to look only at authentication as a binary, static operation; a best practice is to look at authentication as part of a continuous process that integrates static authenticators such as those laid out in SP 800-63B with other signals to deliver continuous, risk-based authentication. Typically, these signals are analyzed as part of an authentication risk engine that helps flag potential anomalies and block efforts to compromise authentication.

- *Provide guidance on security and privacy considerations for the use of behavioral characteristics as an authentication factor.* Our members have seen the market flooded with new solutions here – many of which are very promising, but some of which gather data that may create new security and privacy risks. As NIST considers ways to recognize the use of behavioral characteristics as an authentication factor, the market will benefit from guidance here.

- *Focus on phishing resistance.* Technology and threat have both changed since the publication of SP 800-63-3. Where the 2017 revision flagged concerns about compromises of SMS, attackers have now found ways to phish other AAL2 authentication technologies such as OTP and push-based tools – and as new open-source phishing kits have gotten more sophisticated, this task has become much easier.

  Given how threat has evolved, NIST should be looking to 1) help implementers understand this threat and 2) steer them toward phishing-resistant authentication tools. Continuing to list both phishable and phishing-resistant authentication tools alongside each other will mislead implementers into thinking that these two categories of authenticators are still equivalent in strength or resiliency. Going forward, NIST should adjust its approach to AALs to help implementers clearly differentiate between tools that are phishing resistant and those that are not.

- *Focus on overlapping vulnerabilities.* To the point above: Authentication strength is improved when there are no overlapping vulnerabilities between factors used. However, the ways in which threat actors have evolved over the last few years means that some authentication tools are now vulnerable in ways they were not back in 2017. For example, the fact that memorized secrets and "shared secret" possession-based authenticators such as OTP can both be phished through the same attack vector effectively negates much of the security value of OTP. Arguably, the phishability of many OTP implementations has effectively turned it from a possession-based authenticator to a knowledge-based authenticator. NIST should address new ways that threat has evolved to creates overlapping vulnerabilities among authentication factors.

- *Consider new ways to approach Verifier Impersonation Resistance.* One area we are interested in seeing NIST explore is whether behavioral and/or risk-based tools can be used to address verifier impersonation concerns. Reliance solely on cryptographic tools limits the ability of many organizations to implement Verifier Impersonation Resistance. We would like to see NIST consider whether behavioral tools may also offer some way to address risk here – either as an alternative, or a complement to, existing cryptographic-based tools.

3. General comments

- *Consider a new section focusing on credential management.* Some of our members have highlighted that the current SP 800-63-3 does not fully address issues around credential management. Lifecycle management of authenticators is covered in SP 800-63B, but the issues around lifecycle management in identity go beyond authenticators into credentials – which bind proof of identity to an authenticator. Some elements of credential management are scattered throughout the existing guidance, but a fuller section here may be beneficial to implementers.

- *Consider a new section focusing on authorization and consent.* Issues around how to best capture and communicate consent are getting increasing attention in the identity space. Much of this is being driven by ways in which the privacy landscape has changed since SP 800-63-3 was first published. GDPR has become mainstream, states are passing their own privacy legislation, and Congress is actively working on Federal privacy legislation. All of these laws and rules place a heavy focus on obtaining the consent of an authenticated user.

  While we do not purport to hold a crystal ball revealing what the next five years will bring, we think it is safe to assume that issues around user consent will only be elevated in stature and organizations will be looking for guidance as to how to implement robust consent systems. NIST should consider creating a SP 800-63D that focuses on consent, including its extension and revocation, as well as auditability to be able to demonstrate compliance.

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 Jeremy Grant.