FIDO Alliance Input to the National Institute of Standards and Technology (NIST)

Draft Identity and Access Management Roadmap

June 2023

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on NIST's Draft Identity and Access Management (IAM) Roadmap.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as biometrics and identity verification technologies.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership.

1Password
amazon
AMERICAN EXPRESS
axiad
Bank of America
CVSHealth
Daon
egis Technology
FEITIAN WE BUILD SECURITY
Google
HYPR
IDEMIA
Infineon
intel
JUMIO
LastPass
Lenovo
LINE
mastercard
Meta
Microsoft
nok nok
NTT docomo
OneSpan Be bold. Be secure.
PayPal
PNC
Qualcomm
RAON
RSA
SAMSUNG
THALES
TRUSONA
TRUSTKEY SOLUTIONS
usbank
VISA
vmware
WELLS FARGO
YAHOO! JAPAN
yubico

Overall we are pleased to see NIST publish this new roadmap. Identity and authentication are becoming more complicated – and challenging – each year, as attacks against identity systems continue to get more sophisticated and defenders must find ways to balance better security with privacy, usability, equity, and other factors. Government and the private sector alike both look to NIST for guidance here; each year, the need for NIST leadership grows stronger.

At a high level, we believe NIST has articulated a Roadmap that will address many of the most pressing challenges in IAM.

While our members have a wide range of interests, we are limiting our comments to those areas of the Roadmap that directly relate to FIDO Alliance work in identity and authentication. Below we break down our comments section by section.

Expand and Enhance Biometric and Identity Measurement Programs
Here we believe it would be helpful for NIST to consider adding a new deliverable focused on enhancing biometric technology evaluations to evaluate not just accuracy, but also bias/equity results.

Ongoing questions around bias and equity in biometric systems continue to create material challenges to the use of biometrics in different applications. NIST should look to prioritize work that evaluates not just accuracy but also bias in tested systems; as well as ways to help stakeholders understand the results of this testing in a way that an average layperson can grasp. Doing so will enable both public and private sector implementers of biometric systems to choose products that are both accurate and equitable.

On this topic, we note that FIDO Alliance has recently begun exploring ways to expand the scope of our biometrics certification programs to examine bias in biometric systems; we would welcome the opportunity to partner with NIST here.

Advance Secure, Privacy-Protective, and Equitable Identity Proofing and Fraud Mitigation Options
We believe NIST should consider adding an item to partner with the Department of Homeland Security (DHS) Science and Technology (S&T) directorate to leverage their new initiative to test the performance of different remote ID proofing technologies, with a focus on creating a sustainable approach for testing and certification of these technologies.

As noted earlier, no issue is posing more of a challenge to biometric applications than ongoing questions around bias and equity in biometric systems, and that extends to the use of biometrics in remote identity proofing solutions. DHS S&T has indicated that its new testing of remote ID proofing technologies is intended – for now, at least – to be a one-time round of testing.

However, there is a need for an entity to do ongoing testing of these solutions; FIDO Alliance has launched its own effort to create a program to test and certify these solutions. While the government may decide to rely on its own testing and some point, ideally, inputs and knowledge gained from the government's currently planned one-time testing could feed into ongoing testing and certification efforts run by FIDO (and, for that matter, other non-government entities).

Accelerate the Use of Phishing Resistant, Modern Multi-Factor Authentication
We are pleased to see phishing-resistant MFA listed as one of the core priorities. We offer two comments here:

- The "Build Identity Innovation and Modernization Lab in the NCCoE" deliverable sounds like a lab that would cover issues beyond authentication. We are interested to know if this assumption is correct, and if so, whether this lab should be included in another section?

  Conversely, we believe that the ecosystem would benefit from a NCCoE Lab that focuses – if not wholly, then at least in part – on ways to accelerate the use of phishing-resistant, modern MFA. There is a delta in the US government today between the policies that allow the use of non-PIV authenticators and the types of guidance and reference implementations that can help agencies implement them. A new Lab that focuses on these issues would be very helpful to agencies and the private sector; we expect that many of our members would be interested in collaborating on projects in such a Lab.

  On that note, FIDO Alliance has convened a new workgroup to help tackle the need for additional guidance on the use of FIDO authenticators in a PIV-centric ecosystem; we believe some of the outputs of this workgroup might help to inform the proposed NIST "Implementors Guide to Modern Authentication Technology," as well as any new NCCoE Lab projects that focus on this issue.

- Per our comments earlier this year on the draft of SP 800-63-4: consider integrating key elements of the implementation guidance into the base document, to make it easier for users to comprehend what solutions they should use for phishing-resistant authentication.

Rationale: Today many of the details on what is and is not considered "phishing resistant" are buried in implementation guidance that is separate from SP 800-63B. As we noted in our earlier comments, we continue to hear from implementers who are confused about whether use of FIDO standards is supported in SP 800-63B, and while we point to the Implementation Resources, many implementers never find their way to this document. This causes confusion not just in their organizations, as well as with auditors and regulators.

Modernize the Federal PIV Architecture and Guidance

From the FIDO perspective, the biggest priority here is for NIST to accelerate guidance on ways to support additional phishing-resistant authentication methods, as called for in OMB M-22-09. Much of the work needed here is called out in the Roadmap's section on phishing-resistant MFA. We are pleased with the work underway here, and hope that the new workgroup FIDO Alliance has created to help tackle the need for additional guidance on the use of FIDO authenticators in a PIV-centric ecosystem will produce some deliverables that may be useful inputs to the Special Publications NIST has listed in this section.

We greatly appreciate NIST's consideration of our comments. We look forward to further discussion with NIST on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this response.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.