fido ALLIANCE | simpler stronger authentication

# FIDO Alliance Input to CISA

## Draft Zero Trust Maturity Model and Cloud Security Technical Reference Architecture

October 2021

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the Draft Zero Trust Maturity Model and Cloud Security Technical Reference Architecture published by the Cybersecurity and Infrastructure Security Agency (CISA).

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 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 remote identity verification.

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. Our members include leading firms in banking, payments, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO2 suite of standards – Web Authentication (WebAuthn) and Client to Authenticator Protocol (CTAP) – have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy MFA tools.

As the draft OMB Federal Zero Trust strategy notes, WebAuthn *"is supported today by nearly every major consumer device and an increasing number of popular cloud services."* Apple, Google, and Microsoft have all embedded support for FIDO2 at the device, operating system, and browser level, enabling new models for deployment phishing-resistant MFA to be "built in" rather than "bolted on." The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

The OMB draft articulates a requirement for agencies to use only phishing-resistant MFA for agency, staff, and contractors, and mandates that agencies offer it as an option for all public-facing users. OMB provides a clear rationale for the use of phishing-resistant MFA, noting, *"many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."*

Against this backdrop, our primary comment to CISA on the Draft Zero Trust Maturity Model and Cloud Security Technical Reference Architecture is that while they both discuss the importance of MFA, they say nothing about what kind of MFA should be used, nor do they mention the importance of phishing resistance.

This raises two concerns:

- First, the OMB and CISA documents are inconsistent on the topic of MFA. This inconsistency may cause confusion among implementers who may look to one document but not the other. It will be important for all three documents in this "suite" of Zero Trust guidance to all use consistent language.
- Second, by not calling out the importance of phishing resistant MFA, an implementer relying on the CISA draft may move forward with MFA that is vulnerable to phishing. As the OMB draft notes, all MFA tools do not offer the same levels of security. Over the last six years, attackers have become increasingly proficient in phishing SMS and OTP codes, as well as tricking users into approving login requests sent by push notification. These are attacks that CISA should advise implementers to guard against.

We recommend that the two CISA drafts should be updated to align with the OMB guidance, pointing implementers toward use of MFA that is phishing resistant. Aligning with the OMB guidance that differentiates between different approaches to MFA and requiring phishing-resistant MFA will ensure that government Zero Trust systems cannot be compromised with phishing attacks.

FIDO Alliance also notes that CISA has listed as a "tentative" offering that it will provide *"best practices for agencies looking to use multi-factor authentication to increase the security of identities."* We believe a best practices document on this front would be helpful for implementers, looking perhaps to build on the OMB Zero Trust Maturity Model and pending updates to NIST SP 800-63 and FIPS 201 that will also both – per NIST – focus more keenly on phishing resistance in MFA.

As part of such a document, CISA should consider pointing to use of FIDO-certified authenticators as one way implementers can select phishing-resistance authenticators. This approach has been embraced by other governments such as Australia and the United Kingdom (U.K.), both of whom have not only referenced FIDO standards in their guidance but FIDO certification as well. In 2020, both the Australian and U.K. governments specifically called out FIDO standards and certification programs by name in their MFA guidance.

- The Australian Cyber Security Centre (ACSC) – via its "Essential Eight" guidance on "Implementing Multi-Factor Authentication" – specifically recommends that implementers only use security keys have been certified by the FIDO Alliance.[1]

- The U.K. – as part of its "Using authenticators to protect an online service" guidance (Good Practice Guide 44) published jointly by the Government Digital Service and Cabinet Office– notes that an authenticator token "is high quality if it has been independently tested to prove it meets industry standards, such as the Common Criteria guidelines, FIDO or NIST FIPS 140-2."[2]

FIDO Alliance's certification program has gained this recognition thanks to the robustness and rigor of its program. More than 850 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.[3] Indeed some governments have also pursued their own FIDO certifications – for example, Germany's Federal Office for Information Security (BSI).[4]

[1] See page 5 of https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Implementing%20Multi-Factor%20Authentication%20%28June%202020%29.pdf. Note that this guidance currently references FIDO U2F certification, calling for implementers to *"use U2F security keys that have been certified to the latest U2F specification version."* It is expected that the next revision will shift the focus to FIDO2.

[2] https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services

[3] See https://fidoalliance.org/certification/ for more details on FIDO's certification programs

[4] See https://fidoalliance.org/authenticator-certification-hits-a-new-milestone-with-first-l3/

We believe it will be helpful for agency officials looking to implement WebAuthn and CTAP in accordance with the new OMB Zero Trust guidance to know that they should look for those authentication solutions that have been certified by FIDO Alliance, in line with similar UK and Australia guidance.

We greatly appreciate CISA's consideration of our comments. We look forward to further discussion with CISA 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. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should CISA staff desire to learn more about how FIDO authentication and how its certification programs work.

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