January 22, 2024

To whom it may concern,

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to submit comments on the draft of NIST SP 800-171r3: *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations.*

As background, 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 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, telecommunications, and fintech, as well as those in security, health care, information technology, and government services.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eleven 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 FIDO standards 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 authentication tools.

The importance of phishing-resistant authentication and the role that the FIDO standards play in delivering it have been getting increased attention from the White House and multiple U.S. cybersecurity and regulatory agencies over the last three years. In addition to the White House, NIST, and CISA – not to mention regulators such as the FTC, CFPB, and HHS – all have issued guidance that points to the need for phishing-resistant authentication.

Most notably, the White House called out FIDO in OMB M-22-09, the White House Zero Trust Strategy.[1] Per M-22-09 clearly stated: *"For agency staff, contractors, and partners, phishing-resistant MFA is required."*

The memo went on to discuss how adversaries have found ways to easily compromise some other forms of MFA through phishing attacks, including one-time password (OTP) apps and those authenticators which ask users to approve a login through a push notification, 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.*
>
> *"Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks…the World Wide Web Consortium (W3C)'s open "Web Authentication" standard, another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services.*
>
> *"Web Authentication, also known as WebAuthn, was developed as part of the FIDO Alliance's FIDO2 standards, and is now published by the World Wide Web Consortium (W3C) as a free and open standard.*
>
> *"Public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication. Because most of the general public will not have a PIV or CAC card, agencies will have to meet this requirement by providing support for Web Authentication-based approaches, such as security keys."*

Our concern is that, as currently drafted, NIST SP 800-171r3 appears to 1) conflict with M-22-09 and other government guidance and policies on MFA, and 2) provides implementers with outdated guidance that will fail to protect CUI from phishing attacks.

NIST SP 800-171r3 applies to many firms that are "agency contractors and partners" as defined in M-22-09, yet there is no mention of the need for phishing-resistant MFA in this draft, despite M-22-09 being clear that the use of phishing-resistant MFA is required.

Instead, the draft discusses MFA requirements in section 3.5.3 in more generic terms that

[1] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

do not reflect the vulnerabilities to legacy MFA tools flagged in M-22-09 that have been identified by the White House, CISA, and NIST in other publications.

The closest the draft comes to raising the need for phishing resistance is in section 3.5.4, covering "Replay-Resistant Authentication." While this section reflects some of the concerns about compromises of authentication, the list of "replay-resistant techniques" that are cited are outdated solutions that do not stand up to today's common phishing attacks.

NIST SP 800-63-3[2] coined the term "Verifier Impersonation Resistance" in 2017 to discuss authenticators that can stand up to phishing attacks; NIST has done a great job in the draft of SP 800-63-4[3] in shifting the term to "Phishing (Verifier Impersonation) Resistance," which aligns well with M-22-09, as well as common terminology used in the private sector to discuss the types of MFA solutions which can defend against modern attack vectors.

While Replay Resistance is still mentioned in SP 800-63-3 (and the draft of SP 800-63-4), it has become much less important in the authentication ecosystem and fails to capture threats caused by increasingly sophisticated and scalable phishing attacks now being launched by adversaries.

We understand that SP 800-171 points back to SP 800-53 controls that still incorporate this outdated terminology.[4] However, at a time when threats against MFA have evolved – and the tools we use to defend against these threats have also evolved – it does nobody any good to continue to point organizations who must protect Controlled Unclassified Information (CUI) to language that will not enable those organizations to properly protect this information, and that conflicts with language used by the White House, CISA, and other parts of NIST.

On the CISA front, it is worth nothing that CISA has echoed the White House's messaging with regard to the importance of phishing-resistant authentication in the advisories it is putting out to the private sector, stating:

> *"Not all MFA methods gives you the same level of protection. Some MFA types are better than others—phishing-resistant MFA is the standard all industry leaders should strive for, but any MFA is better than no MFA. You should still strive to implement stronger MFA to avoid being hacked.*

---

[2] See Section 5.2.5 at https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

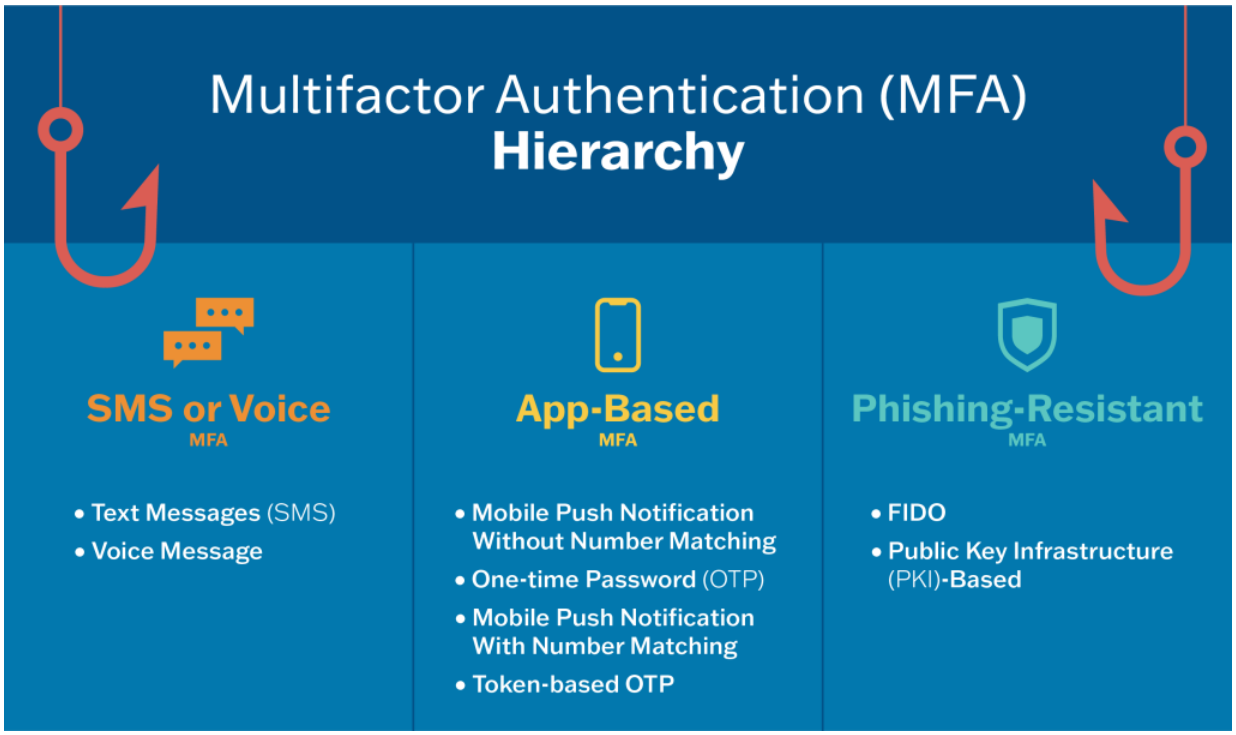
[3] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.ipd.pdf

[4] To that point, we are somewhat puzzled as to why SP 800-53 Rev 5 did not incorporate updates to align with SP 800-63-3 on requirements for Verifier Impersonation Resistance – and urge NIST to address this omission.

- *The only widely available phishing-resistant authentication is FIDO/WebAuthn authentication. CISA urges all organizations to start planning a move to FIDO because when a malicious cyber actor tricks a user into logging into a fake website, the FIDO protocol will block the attempt. See CISA Fact Sheet Implementing Phishing-Resistant MFA, CISAJen's blogpost Next Level MFA: FIDO authentication, and the Fido Alliance's How Fido Works for more information.*
- *If you can't currently implement phishing-resistant MFA, consider using numbers matching MFA to block mobile push bombardment and SMS-based attacks. See CISA Fact Sheet Implementing Number Matching in MFA Applications for more information."*

CISA has called FIDO the "gold standard" for MFA; it has also created a graphic depicting their "MFA Hierarchy" to help assist implementers as they make choices on what types of MFA to implement, and guiding them toward phishing-resistant authentication.

At a time when CISA is guiding private sector organizations of all sizes toward the use of phishing-resistant MFA – as are other parts of NIST – NIST guidance to those parties who must protect Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations should be aligned.



Contractor IT systems are in many cases a de-facto extension of U.S. government systems, given the high reliance of agencies on contractors to support a variety of agency mission requirements. And just as adversaries are actively targeting agency IT systems, they are also targeting contractor IT systems. Indeed, one of the most devastating breaches in American

history – the 2015 breach of the Office of Personnel Management (OPM) – was caused by foreign adversaries compromising an authenticator at an OPM contractor.

Given the rash of reports emerging each month about major data breaches linked to the compromise of legacy authentication tools such as those using OTPs or push notifications, it is imperative that agencies ensure all of their contractors are using phishing-resistant MFA, and that NIST SP 800-171r3 is updated to include this security requirement.

We greatly appreciate consideration of our comments. We look forward to further discussion 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 letter.

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