FIDO Alliance Comments to the U.S. OFPP, GSA, DoD and NASA

July 2026

Proposed Amendments to the Federal Acquisition Regulation (FAR) – FAR Case 2026-001

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to provide input to the Office of Federal Procurement Policy (OFPP), Office of Management and Budget (OMB); Department of Defense (DoD); General Services Administration (GSA); and National Aeronautics and Space Administration (NASA) on its proposed amendments (FAR Case 2026-001) to the Federal Acquisition Regulation (FAR).

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 phishing-resistant Multi-Factor Authentication (MFA) and passwordless authentication.

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.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the 14 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 – such as passkeys and security keys – that are both more secure and also easier to use than legacy authentication tools.

As we detail in the pages that follow, the importance of phishing-resistant authentication such as that using the FIDO standards or PKI has been recognized – and in some cases, embedded in policy as a formal requirement – by the Office of Management and Budget (OMB), NIST, CISA, and Congress. This update of the FAR – and the creation of Standard Form XXX to address controls around Controlled Unclassified Information (CUI) – provides an ideal opportunity for the government to also embed a requirement for phishing-resistant authentication into every contract that the Federal government enters into which involves access to CUI.

However, as we detail below, current NIST guidance on CUI (NIST SP 800-171) has yet to be updated to reflect requirements in the Federal government's Zero Trust Strategy (M-22-09) that require contractors to use phishing-resistant MFA. Thus, any effort to embed SP 800-171 controls into the FAR will fail to address

a critical vulnerability in many authentication tools used by contractors unless:

1) NIST first is directed to update SP 800-171 to reflect current Federal policy on authentication or,
2) the FAR includes language directly on phishing-resistant authentication.

We include recommendations on how the government can address both of these issues below.

The importance of phishing-resistant authentication and the role that the FIDO standards play in delivering it have been getting increased attention from multiple U.S. cybersecurity and regulatory agencies over the last four years.

- OMB called out FIDO authentication in OMB M-22-09, the Federal government's Zero Trust Strategy.[1] 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 compromises 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."*

  The memo also noted that while *"the Federal Government's Personal Identity Verification (PIV) standard is one such approach"* to delivering phishing-resistant authentication, *"PIV will not be a practical option for some information systems and situations."* For this reason, it expanded the focus on authentication beyond PIV to encompass other types of phishing-resistant authentication, stating:

  > *"Agencies are permitted under current guidance to use phishing-resistant authenticators that do not yet support PIV or Derived PIV (such as FIDO2 and Web Authentication-based authenticators) in order to meet the requirements of this strategy."*

  Note that the focus on contractors was quite deliberate in M-22-09, given that 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

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

at an OPM contractor. More recently, researchers discovered that a CISA contractor "with administrative access to the agency's code development platform had created a public GitHub profile called "Private-CISA" that included plaintext credentials to dozens of internal CISA systems."[2]

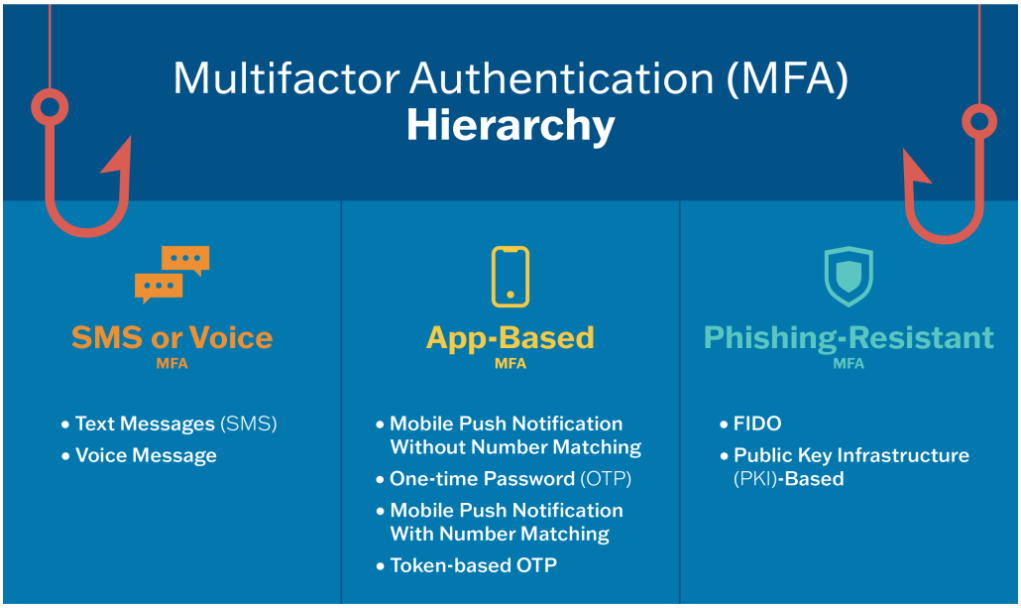
Also of note, the U.S. Senate just included a requirement for DoD to use only phishing-resistant authentication (per section 1638 of the FY27 National Defense Authorization Act) out of concerns that DoD was falling behind civilian agencies in its lack of a requirement on this issue.

- CISA has also echoed OMB's messaging, 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.

  - *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.*
  - *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.



[2] See https://krebsonsecurity.com/2026/05/lawmakers-demand-answers-as-cisa-tries-to-contain-data-leak/

Despite the requirement in M-22-09 for agency staff, contractors, and partners to use only phishing-resistant MFA, NIST has not updated SP 800-171 to reflect this requirement.

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 the document, despite M-22-09 being clear that the use of phishing-resistant MFA is required.

Instead, SP 800-171r3 discusses MFA requirements in section 03.05.04 in more generic terms that do not reflect the vulnerabilities to legacy MFA tools flagged in M-22-09 that have been identified by OMB, CISA, and NIST in other publications.

The closest SP 800-171r3 comes to raising the need for phishing resistance is in section 03.05.04, 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. At a time when generative AI is leading to a sharp increase in phishing attacks targeting weak authentication solutions – phishing attacks are up 4151% since ChatGPT was introduced in late 2022 – it is imperative that this guidance be updated to address current threat vectors.[3]

NIST's Digital Identity Guidelines (SP 800-63-4) are much more up to date. NIST focuses significant attention on "Phishing (Verifier Impersonation) Resistance," including a requirement that "*Federal agencies SHALL require their staff, contractors, and partners to use phishing-resistant authentication to access federal information systems.*"[4] This language aligns with M-22-09.

While Replay Resistance is still mentioned in 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. 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 OMB, CISA, and other parts of NIST.

The draft controls for FAR Case 2026-001 include a requirement for strong authentication around HSPD-12/FIPS 201, but it only addresses part of the phishing-resistant authentication challenge. This language should be amended to ensure that any authentication that does not use PIV cards is still phishing-resistant.

The proposed language in both FAR 4.205 and FAR 52.204-9 includes text that impacts authentication.

FAR 4.205 reads:

> *4.205 Personal identity verification.*
>
> (a) Agencies must include their implementation of Homeland Security Presidential Directive-12 and the Federal Information Processing Standards Publication (FIPS PUB) Number 201 in solicitations

[3] See https://www.dashlane.com/blog/genai-fuels-phishing-sophistication
[4] https://pages.nist.gov/800-63-4/sp800-63b.html#AAL_SEC4

and contracts that require the contractor to have routine physical access to a Federally-controlled facility and/or routine access to a Federal information system. For information on personal identity verification (PIV) products and services see http://www.idmanagement.gov.

(b) When acquiring PIV products and services not using the GSA Federal Supply Schedule for HSPD-12 Product and Service Components, agencies must ensure that the applicable products and services are approved as compliant with FIPS PUB 201 including—

(1) Certifying the products and services procured meet all applicable Federal standards and requirements;

(2) Ensuring interoperability and conformance to applicable Federal standards for the lifecycle of the components; and

(3) Maintaining a written plan for ensuring ongoing conformance to applicable Federal standards for the lifecycle of the components.

FAR 52.204-9 reads:

52.204-9 Personal Identity Verification of Contractor Personnel.

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(d) The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

As noted earlier, PIV cards provide excellent authentication security where they can be used across government, in that they also deliver phishing resistance.

However, as noted earlier, M-22-09 stated, *"PIV will not be a practical option for some information systems and situations,"* in large part because the PIV platform does not easily work well with mobile devices or some modern applications and platforms. For this reason, OMB stated *"Agencies are permitted under current guidance to use phishing-resistant authenticators that do not yet support PIV or Derived PIV (such as FIDO2 and Web Authentication-based authenticators) in order to meet the requirements"* of M-22-09.

Against this backdrop, it would make sense for the proposed language in FAR 4.205 and 52.204-9 to be amended with new language to reflect M-22-09, as well as the broader threat landscape.

We suggest the following new subsection (c) for FAR 4.205:

(b) Agencies must include language in solicitations and contracts to require that a contractor use only phishing-resistant authentication when accessing a Federal information system or CUI. PIV products and services address this requirement, as do other authentication solutions that meet requirements for phishing resistance as defined by NIST in Section 3.2.5 of SP 800-63B-4.

Additionally, we suggest that a new subsection (e) be added to FAR 52.204-9:

> (e) For contractor employees granted routine access to a Federal information system, the Contractor shall, in addition to the personal identity verification procedures in paragraph (a) of this clause, use only authentication solutions that meet requirements for phishing resistance as defined by NIST in Section 3.2.5 of SP 800-63B-4.

With this, paragraph (d) of FAR 52.204-9 should be amended to reflect this new section, reading:

> (d) The Contractor shall insert the substance of this clause, including this paragraph (d) and paragraph (e), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

Note that we suggested a standalone new paragraph (e), rather than amending paragraph (a) directly, so the existing PIV/HSPD-12 requirement in (a) remains untouched and the new phishing-resistant authentication requirement layers on top of it as a distinct obligation.

These minor changes would bring the FAR in line with M-22-09, as well as commonly accepted best practices for cybersecurity.

We also believe it would make sense to cross-reference this language into the new FAR Part 40 (specifically Subpart 40.3—Safeguarding Information) so that the Council's consolidated safeguarding-information framework and its identity-authentication requirement do not drift apart the way 52.204-9 and M-22-09 already have.

We appreciate the government's considerations of our comments and suggestions. We would welcome the opportunity to provide the Council with technical input on authenticator standards as this rule moves toward a final version. Should you have any questions on our submission – or would like to learn more about FIDO standards and certification programs – please reach out to our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our policy advisor, Jeremy Grant, at jagrant@venable.com.