FIDO Alliance Comments to the U.S. Department of War

August 2026

RFI on Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to provide input to the Department of War (DoW) on its RFI on "Reforming Cybersecurity Maturity Model Certification (CMMC) and Reducing Compliance Burden for the Defense Industrial Base (DIB)."

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.

While we are not a contractor or vendor to DoW itself, many of our members support the Department with technology and services in the cybersecurity realm. Given this – and the criticality of phishing-resistant authentication to the security of our digital systems – we believe it is important to respond to this RFI.

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.

We greatly appreciate that the DoW CIO highlighted the importance of phishing-resistant authentication in last month's "Brilliant at the Basics" campaign – listing phishing-resistant MFA as the number one control for DIB partners. As DoW rethinks CMMC Phase II requirements, our message is a simple one: ensure that phishing-resistant MFA remains a critical control for DIB partners in any revised approach to CMMC.

With this, we offer four core points for consideration. Collectively, they address both question 2 (Which specific security controls has your organization found to deliver the most tangible uplift of cybersecurity and actual risk reduction?) and question 7 (7.What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically improve operational resilience against cyber attacks at your organization?).

1) **Phishing-resistant MFA is a critical control.**
   While legacy MFA tools were once effective at blocking most attacks on authentication systems, attackers have caught up. Today most adversaries are able to phish not just passwords, but also the outputs of legacy MFA tools such as OTPs and push-notification-based authenticators – and they are doing it at scale.

   The emergence of generative AI tools have helped to supercharge the frequency and efficacy of these attacks: Since the

launch of ChatGPT in Q4 2022, phishing attacks have reportedly increased by more than 4,100%.[1] Many of the authentication controls that worked well ten years ago are now vulnerable, and this issue is especially important in the DOW and across the DIB.

CISA documented the impacts of these vulnerabilities extensively in its 2023 CSRB report on "Attacks Associated with LAPSUS$ and Related Threat Groups, which focused heavily on why it is a national imperative to move to phishing-resistant MFA.[2] OMB in its 2022 Federal Zero Trust Strategy (M-22-09) required all Federal employees and contractors to use only phishing-resistant MFA, although this requirement did not directly apply to national security systems. And NIST has updated its digital identity guidelines (SP 800-63-4) to highlight the importance of phishing-resistant MFA – both FIDO and PKI-based – and the requirement for high-assurance applications in government to use it.

2) **DoW pioneered the use of phishing-resistant MFA – but much of the DIB still uses legacy, phishable authenticators.**
Over 25 years ago, the then-Department of Defense pioneered the use of phishing-resistant MFA in government with the introduction of the Common Access Card (CAC) and its PKI credentials; DISA documented in 2006 that use of the CAC and PKI had reduced network intrusions by 46%.[3]

However, there are many places where the CAC and/or PKI credentials cannot be easily used, and where the fallback authentication solution is legacy phishable MFA, or sometimes just a password. This is particularly an issue with use cases involving mobile devices, people who bring their own device, legacy applications that do not easily integrate with CAC or PKI, as well as those involving specialized equipment that cannot support a CAC reader. Likewise, many DIB partners do not have a CAC or a similar authenticator and thus fall back to other authentication tools including many that are phishable.

This challenge was explicitly called out in M-22-09 in its discussion around the personal identity verification (PIV) card platform, which noted: *"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.

Security can be meaningfully improved across the DIB by implementing phishing-resistant MFA such as FIDO security keys or passkeys. We note that a number of security key vendors have obtained FIPS 140 validation; some are able to support both the FIDO standards and the PIV standards – enabling an individual to carry multiple phishing-resistant authentication tools in a single hardware key.

3) **NIST SP 800-171 does not include any reference to phishing-resistant MFA.**
NIST SP 800-171 Rev 2 – which is the current baseline for CMMC compliance – does not include any reference to phishing-resistant MFA, nor does its successor, NIST SP 800-171 Rev 3. The fact that the most recent revision of this guidance did not include this requirement is especially notable, given that it was published over two years after OMB published the Federal government's Zero Trust Strategy (M-22-09) that stated "*For agency staff, contractors, and partners, phishing-resistant MFA is required."*

We highlight this as one example of where a compliance-based approach to CMMC may fail to achieve tangible security outcomes, given the gap between current known threats and the controls called out in these SPs.

Our understanding is that NIST may soon update SP 800-171 to address this concern, however, for the time being, the authentication advice in DOW's "Brilliant at the Basics" guidance is more relevant and up to date than NIST's current guidance on protecting CUI.

4) **Quickly uplifts operational resilience with minimal burden.**
Every major operating system, platform, and browser has built in support for the FIDO standards – enabling DIB organizations of all sizes to easily implement phishing-resistant authentication without material complexity or investment. Given that credential compromise remains a major threat vector across the DIB, FIDO authentication offers a low-cost and efficient way for DIB organizations to materially improve their security posture.

[1] See https://www.dashlane.com/blog/genai-fuels-phishing-sophistication
[2] See https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
[3] As noted at https://www.nextgov.com/cybersecurity/2007/01/cac-use-nearly-halves-dod-network-intrusions-croom-says/231194

As an added signal that demonstrates the maturity of the FIDO standards, FIDO Alliance estimates that 5 billion passkeys – built off of the FIDO standard – are now used worldwide.[4]

Additionally, nearly 1500 authentication products have been certified by the FIDO Alliance as meeting FIDO standards – ensuring that there is a large ecosystem of providers that DIB organizations can choose from, should they be asked as part of any revised approach to CMMC to implement phishing-resistant authentication.

We appreciate the government's considerations of our comments and suggestions. 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.

FIDO Alliance
3855 SW 153rd Drive
Beaverton, Oregon 97003 USA
+1 (503) 619-2683

[4] [4] As noted at https://fidoalliance.org/fido-alliance-reports-accelerating-global-passkey-adoption-on-world-passkey-day-2026/