yubico

# Meeting Zero Trust and phishing-resistant MFA requirements in Memorandum 22-09

## Impact of Executive Order 14028 and OMB M-22-09

Per the guidance of the May 12, 2021 White House Executive Order 14028 on Improving the nation's cybersecurity, on January 26, 2022, the Office of Management and Budget (OMB) M-22-09 memorandum set forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives including a new baseline for access controls across the government that prioritizes defense against sophisticated phishing attacks.

The memo requires that federal agency staff, contractors, and partners use phishing-resistant multi-factor authentication (MFA) to reduce the threat from sophisticated attacks. Phishing-resistant MFA is required to be used for all authentication, whether in the cloud or on a traditional network. Additionally, the memo expects agencies to use cloud-based infrastructure, and offer phishing-resistant MFA options for public-facing digital services. The memo requires these cybersecurity standards to be deployed by the end of fiscal year 2024.

While OMB M-22-09 is focused toward federal agencies, it's imperative for state and local government, education, and private sector organizations to follow suit, to ensure the nation's cybersecurity is protected.

## Importance of phishing-resistant MFA in M-22-09

The reason for this mandate is that sophisticated attackers can intercept legacy forms of authentication, such as mobile-based authenticators, that are highly susceptible to phishing, malware, SIM swaps, and man-in-the-middle (MiTM) attacks.

**M-22-09**

mandates federal agencies to discontinue using authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications.

The memo highlights two phishing-resistant approaches to MFA that can defend against these attacks:

- The Federal Government's Personal Identity Verification (PIV) standard that smart cards are built on, which has long been used to provide access to on-premises environments and is widely supported.
- The WebAuthn/FIDO2 standard that is supported today by nearly every major consumer device, and an increasing number of popular cloud services. FIDO2 is the overarching term for FIDO Alliance's set of specifications, of which WebAuthn is a key specification. WebAuthn can be used in combination with a FIDO2 security key for phishing-resistant MFA.

PIV and WebAuthn/FIDO2 are the proven standards offering phishing-resistant MFA.

> FIDO stands for "Fast IDentity Online" and is considered the gold standard of multi-factor authentication.
>
> CISA

## Achieving phishing-resistant MFA guidelines in M-22-09

### 1. Authenticator considerations

An important component of phishing-resistant protocols is the use of public/private key cryptography and the criticality of protecting the key material. Device authenticators play an important part in protecting the key material. As a result, for government use, smart cards that use the PIV standards and security keys that use the WebAuthn standard must be FIPS validated. Devices that are FIPS validated have been independently validated by a NIST specified laboratory as meeting specific security requirements and are listed on NIST's Cryptographic Module Validation Program site. If the product is not listed on the site, then it is not FIPS validated.

**The YubiKey 5 FIPS Series**
From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

Yubico offers the YubiKey—the best available security against phishing attacks and account takeovers with PIV and WebAuthn modules on the same key. YubiKeys are FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines. YubiKeys are DFARS/NIST SP 800-171 compliant, and are approved for use in DOD Non-Classified and Secret Classified Environments.

The YubiKey is simple to deploy and use—YubiKeys can be used across legacy and modern applications, services, and devices, with multi-protocol support for SmartCard, OTP, OpenPGP, FIDO U2F and WebAuthn/FIDO2 on a single key. YubiKeys are supported natively by leading identity, credential and access management (ICAM) solutions such as Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, OneLogin, Ping Identity platform, and RSA SecurID® Suite, and provide highest-assurance security for non PIV/CAC eligible employees and contractors, teleworkers, cloud services, isolated/closed networks, digital citizen services, and mobile device users.

### 2. Deciding between PIV and WebAuthn/FIDO2

To achieve phishing-resistant MFA across any and all access points used by employees, contractors and partners—whether in-person, hybrid, or remote, within the timeframe set forth in the memo, agencies can leverage PIV and/or WebAuthn/FIDO2 deployments. These standards also need to be an option offered to end-customers for public-facing digital services.

Leveraging solutions based on PIV and WebAuthn/FIDO2 will allow you to more easily meet the requirement due to the interoperability of standards compared to using proprietary solutions. Depending on your solutions provider's offerings, WebAuthn/FIDO2 can be used for on-premises access, and PIV can be used for cloud access as well.

Your first step should be to understand your access points and how they support these standards, to ensure you have the necessary phishing-resistant coverage.

Many commonly used access points such as VPNs (Virtual Private Network), IDPs (Identity Provider), cloud platforms, desktop login, and web access offer support today either for webAuthn, PIV, or both. The chart below shows an example of common access points that support phishing-resistant MFA using either WebAuthn/FIDO2, or PIV, as well as YubiKey support. Check with your technology partners to validate their capabilities.

## Phishing-resistant authentication options

| Access points | | Offers webAuthn support | Offers PIV support | YubiKey (webAuthn/FIDO and/or PIV) |
|---|---|---|---|---|
| On premise (active directory) | Windows 10+ Login | ✓/ 3rd party | ✓ | ✓ |
| | Earlier versions of Windows Login | 3rd party | ✓ | ✓ |
| | macOS Login on a Windows domain | 3rd party | ✓ | ✓ |
| | VPN Access | Varies | ✓ | ✓ |
| | Secure Proxy Gateways | ✓ | Varies | ✓ |
| Cloud platforms | Microsoft Azure | ✓ | Preview / Federation | ✓ |
| | Amazon Web Services (AWS) | ✓ | ✓/ Federation | ✓ |
| | Google Cloud | ✓ | Federation | ✓ |
| | Oracle Cloud | ✓ | Federation | ✓ |
| | IBM Cloud | ✓ | Federation | ✓ |
| IDPs | Okta | ✓ | ✓ | ✓ |
| | Ping | ✓ | ✓ | ✓ |
| | DUO | ✓ | N/A | ✓ |
| | ForgeRock | ✓ | ✓ | ✓ |

## Seamlessly procure and distribute YubiKeys at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

## Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator. YubiKeys are produced in the USA, maintaining security and quality control over the entire manufacturing process.

**About Yubico** As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

**Yubico AB**
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

**Yubico Inc.**
5201 Great America Pkwy, Suite 122
Santa Clara, CA 95054
844-205-6787 (toll free)
650-285-0088