yubico

YUBICO WHITE PAPER I SEPTEMBER 2021

Best practices to secure government teleworkers with the YubiKey

A modern PIV/CAC alternative

Contents

Executive summary

COVID-19 changed the way government employees worked and accelerated digital transformation to ensure continuity of operation. This required the government to address the shortfalls in existing IT infrastructure and authentication to ensure data security and mission continuity, and stay protected against malicious cyber actors and nation states.

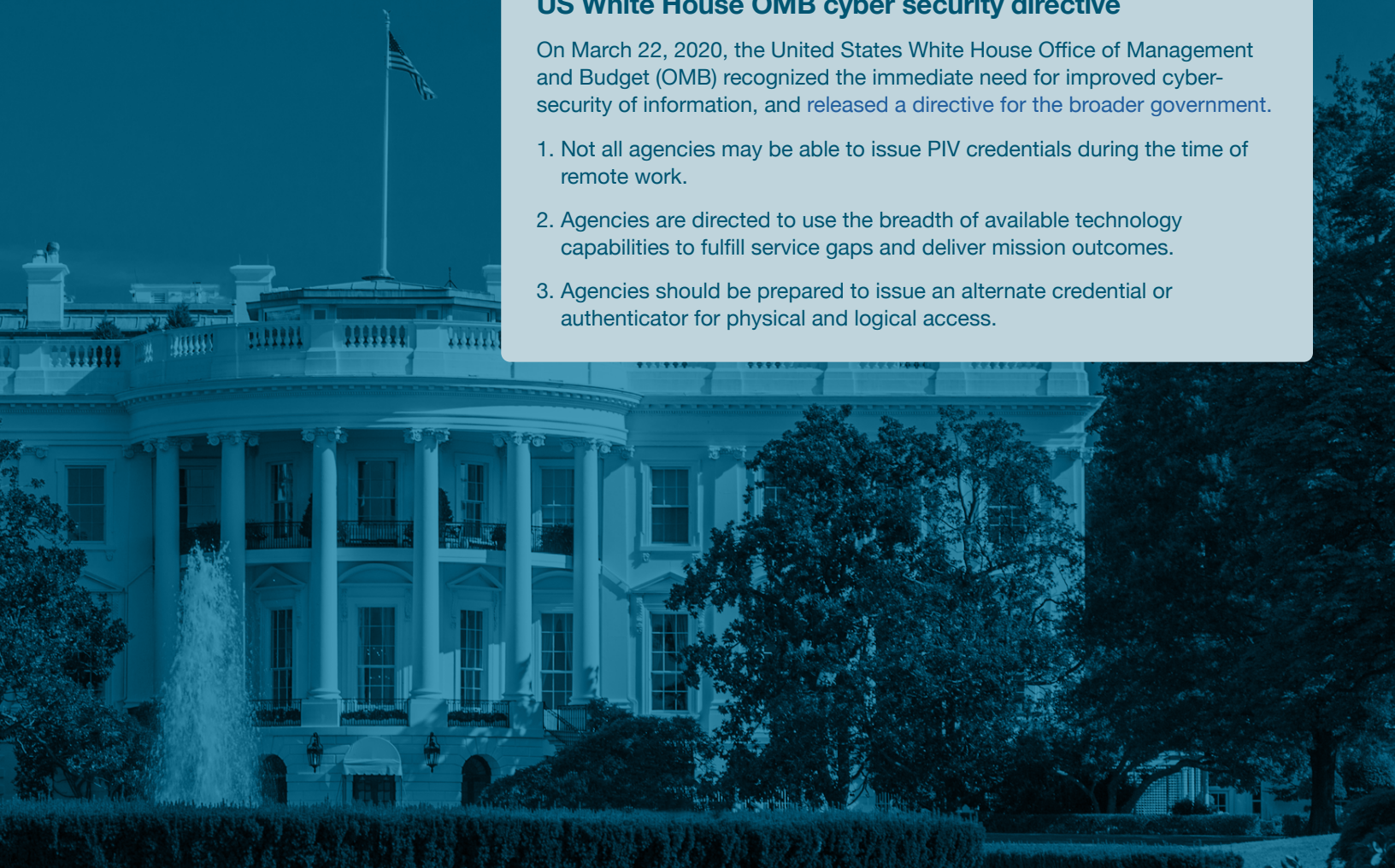
Prior to COVID-19, government agencies like many other organizations, relied on a perimeter security framework and teleworking was the exception, not the rule. COVID-19 forced thousands of employees to telework from geographically dispersed environments and since then, many continue to telework based on their roles and responsibilities.Today, there's a proliferation of personal technologies such as non-government approved personal computers and personal mobile devices being used to connect to unclassified networks. The perimeter and end-points have dramatically shifted today and in the future, and the threat to remote workers and to the information exchanged over their connections remains as high as ever.

For the Department of Defense (DOD) and other federal, state and local government agencies, teleworkers, including remote and hybrid workers, introduce new potential vulnerabilities—whether it be weak passwords on personal computers not being updated with the latest vendor security patches, poorly secured home WiFi routers, or a family member's device passing along a computer virus.

US White House OMB cyber security directive

On March 22, 2020, the United States White House Office of Management and Budget (OMB) recognized the immediate need for improved cyber-security of information, and released a directive for the broader government.

1. Not all agencies may be able to issue PIV credentials during the time of remote work.
2. Agencies are directed to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes.
3. Agencies should be prepared to issue an alternate credential or authenticator for physical and logical access.



Why it matters:

The need for secure PIV/CAC alternatives

Government agencies and Defense Industrial Base (DIB) partners need to strengthen cyber security capabilities on their networks for remote and hybrid workers, particularly in authentication of users joining the Department of Defense (DoD) and DIB networks. Agencies can use alternate credentials or authenticators currently approved by the DoD Chief Information Officer (CIO) to address this urgent need to replace or augment existing PIV and CAC capability. This is particularly beneficial for access to legacy and networks where PIV and CAC are currently not viable alternatives (i.e., legacy systems that workers need to access to continue their work).

PIV and CAC rely on a centralized identity and in-person proofing model where identities are validated in-person prior to credentials being issued, which may not be doable at certain times. Additionally, PIV and CAC authentication infrastructure lacks the convenience and flexibility required to support a rapid shift to remote and hybrid work environments. Many employees do not have PIV and CAC readers at home. There may also be contractors, sub-contractors, and coalition partners that aren't eligible for these credentials, or for access to legacy networks that cannot be PIV/CAC enabled. When usernames and passwords are used in lieu of token based multi-factor authentication (MFA), unnecessary risk is introduced from potentially unsecured home networks to the broader networks they are connecting to.

US White House May 12, 2021 Executive Order 14028

In response to the 2020 SolarWinds attack the Biden Administration released Executive Order 14028. The executive order recognizes the importance of MFA and how it greatly deters account compromise. It mandates that agencies shall adopt impersonation-resistant MFA within 180 days.

To address this, agencies can leverage funding appropriated by Congress from the Technology Modernization Fund (TMF), and for shared services provisioned by the Cybersecurity and Infrastructure Security Agency (CISA) while prioritizing cyber security in their annual budget requests.

The solution:

Secure government teleworkers against phishing and other cyber security threats with the YubiKey

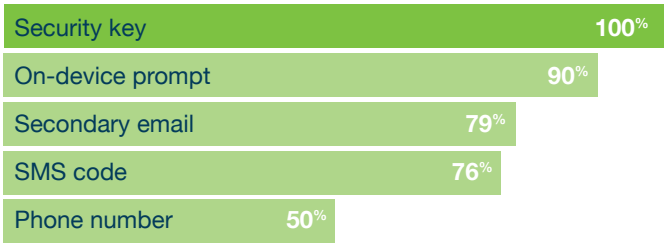
Traditional MFA methods are insecure and do not offer the best user experience. SMS, one time passwords, and even mobile push authenticators are susceptible to account takeover attacks from phishing and man-in-the-middle attacks. YubiKeys have been proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks.

YubiKeys offer the best of both worlds–the strongest security against phishing attacks and account takeovers, as well as the best user experience. To authenticate, users simply tap/touch their security key. YubiKeys do not require batteries, have no breakable screens, do not need a cellular connection, and are water-resistant and crush-proof.

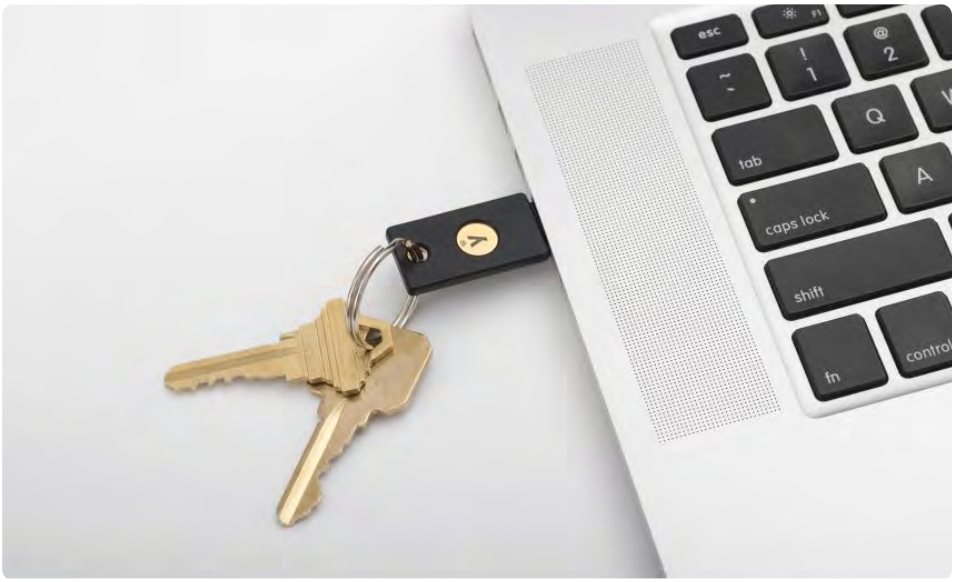
YubiKeys feature modern protocols like FIDO2 and WebAuthn, as well as OTP, SmartCard (PIV), OpenPGP, earlier FIDO versions, and more. A single key supports multiple applications, allowing YubiKeys to work with current applications and authentication methods, and advanced and emerging protocols at the same time.

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.

Account takeover prevention rates



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.



The benefits:

The benefits: YubiKey as a modern PIV/CAC alternative for highest-assurance MFA for government teleworkers

The YubiKey from Yubico provides a government-approved MFA solution for securing remote and hybrid workers, that complies with the highest industry standards. The Yubikey is one of only three DoD CIO government approved alternate authenticators that meet DoD's rigorous cybersecurity requirements.

Fast Identity Online (FIDO) security keys like the YubiKey provide an immediate, affordable solution and are available to implement at scale today. DoD CIO guidance and approval for use of YubiKey was released as early as 2018, demonstrating that the US government recognized the need for agile, adaptable, scalable and affordable security solutions far long before COVID-19. In addition, the successful implementation of YubiKeys in DoD was enhanced by its proven track record of being easy to use, an important aspect for successful adaptation across an enterprise.

YubiKeys comply with the highest standards and can be rapidly deployed to government teleworkers

YubiKeys provide the highest-assurance authentication security and serve as a modern PIV/CAC authentication alternative for government agencies.

With a hardware key USB-A, USB-C, 5Ci and NFC form factors that doesn't require a specialized reader, and the ability to mail keys directly to residential addresses across more than 30 countries, YubiKeys offer the strongest authentication security solution and can be rapidly and easily deployed to remote government workers.

YubiKeys are:

- FIPS 140-2 certified (Certificate #3914) Overall Level 2, Physical Security Level 3
- Validated to NIST SP 800-63-3 Authenticator Assurance Level (AAL) 3 requirements
- Supported for DFARS/NIST SP 800-171
- WebAuthn/FIDO/FIDO2 compliant
- Approved for use in DOD Non-Classified and Secret Classified environments
- In compliance with Homeland Security Presidential Directive 12 (HSPD 12)

YubiKey is an affordable solution that enables a wide variety of end user device utilization

YubiKeys accommodate derived PIV/CAC requirements, eliminating device-based authentication and minimizing Bring your Own Device/Bring your own approved device (BYOD/BYOAD) reimbursement costs. A single security key can be used to securely authenticate users to applications and services across multiple government issued or approved personal devices such as laptops, desktops, tablets, and mobiles, making it a cost-effective solution.

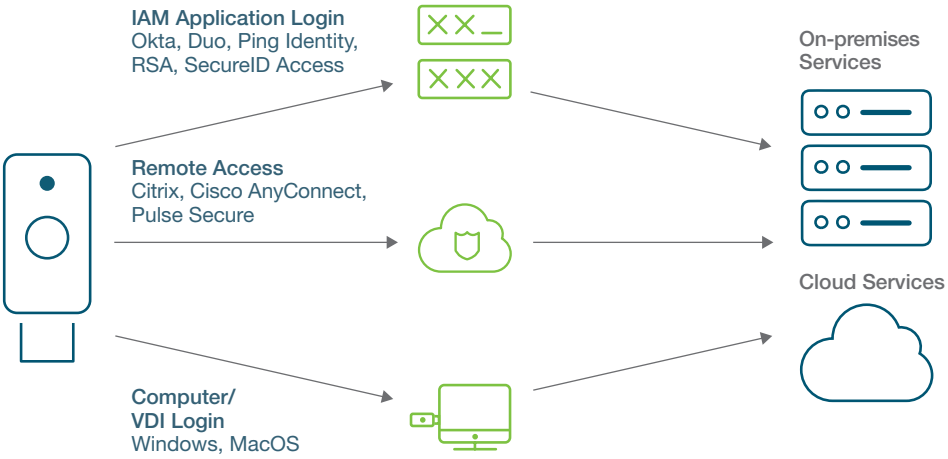
YubiKey has a trusted United States (US) based supply chain

Manufactured securely in the US using stringent processes and a secure supply chain for trustworthy components, YubiKeys are fully vetted and approved for sale throughout the public sector.

Best practices:

5 ways YubiKeys can be used to protect government teleworkers using highest-assurance MFA

How the YubiKey helps secure government teleworkers



1 Enable MFA for identity access management (IAM) systems and identity providers (IdPs)

The best cloud and hybrid environments leverage IAM solutions to enable employees to work without the hassle of multiple usernames and passwords. Many of the leading IAM vendors offer native YubiKey support including Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID Suite, and others. Agencies can immediately improve the level of security across the entire organization by simply turning on MFA with YubiKeys. IAM vendors and IdPs can also be used for Single Single On (SSO) to other business critical messaging or video conferencing apps such as Microsoft Teams, Google Hangouts, and Zoom.

2 Secure VPN access with MFA

Securing access to VPN for government teleworkers is a key step in securing the network against malicious actors. Pulse Secure and Cisco AnyConnect, can be configured to work with a YubiKey as a smartcard (PIV) for remote access. Other VPN applications that offer native support for YubiKeys use the one-time password (OTP) capabilities.

3 MFA for computer login

Whether employees are using a Mac or Windows machine, there are several options for securing computer logins with the YubiKey. One of the most effective ways is to leverage the smart card functionality of the YubiKey, and use the key in addition to a PIN, to lock down access to a computer. Most recently, Yubico has been working very closely with Microsoft to enable native YubiKey support in Microsoft Azure Active Directory for a FIDO-based passwordless login experience.

4 Step-up authentication for password managers

A recent Ponemon Institute report showed employees manage passwords with sticky notes and human memory. Whether employees are remote workers or not, they need a simple and safe way to create, store, and manage passwords. The YubiKey integrates with several enterprise-grade password managers including 1Password, Dashlane, Keeper Security, LastPass, and more.

5 Securely generate one-time time-based passcodes

Many of the services or applications being used at various agencies may support time-based one-time passcodes (OTPs) — such as Google Authenticator or Authy — as a two-factor authentication method. The Yubico Authenticator application and a YubiKey can replace those authenticator apps. Instead of the one-time passcodes being stored within a mobile device or computer, secrets are stored in the YubiKey. This allows users to generate OTP codes within the app by inserting or tapping the YubiKey to a device. Yubico authenticator is compatible with iOS, Android, Windows, and Mac.

Telework is here to stay

As government agencies consolidate real estate holdings and offer more flexible working to employees based on their job role and functions, remote and hybrid work will continue into the future. Government agencies need to fast-track secure easy-to-use authentication to ensure that remote workers connecting to government networks and cloud-hosted services do not leave open doorways for cyber criminals to exploit. By mitigating cyber security threats such as spear phishing, malware, and man-in-the-middle attacks with FIPS validated hardware security keys such as the Yubikey, will help agencies ensure the security and confidentiality of their networks and information.

For more information on the YubiKey as a federally-approved authentication solution to protect government teleworkers, watch the on-demand panel discussion Telework Impact on Cybersecurity across the federal government with Ross Foard, Senior Engineer Cybersecurity Division Cybersecurity and Infrastructure Agency (CISA); Lisa Palma, Cybersecurity Specialist Identity and Access Management, US Department of International Development; Joe Ramsey, CISO/Director of IT Security, International Trade Administration, US Department of Commerce; and Jeremy Grant, formerly Senior Executive Advisor, National Institute of Standards and Technology.

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.