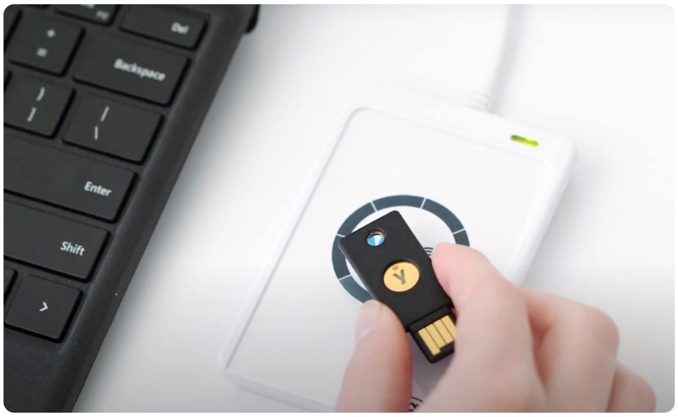
yubico

The future of Federal cybersecurity is here

What every agency needs to know about smart cards simplified



New mandates impact every Federal agency

Get ready for federal cybersecurity to undergo the biggest upheaval yet. In the wake of the SolarWinds attack, which breached nine federal agencies, the Biden administration issued Executive Order #14028 in May 2021. This order requires every federal office to make sweeping cybersecurity upgrades, starting now.

Specifically, the Executive Order and the related Office of Management and Budget (OMB) memo M-22-09 mandates immediate adoption of phishing-resistant multi-factor authentication (MFA), specifically mentioning that legacy MFA approaches such as SMS/voice calls, one-time codes, or push notification to protect access should not be employed. And while some offices are closer to meeting the mandate than others, everyone will need to review, and in many cases, improve how they handle cybersecurity.

For those responsible for federal cybersecurity, the urgent question becomes how to comply with the EO using the least amount of time, budget, goodwill and other resources necessary?

EO #14028 and M-22-09

mandate 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.

Why traditional smart cards aren't enough anymore

A pillar of federal cybersecurity for more than 20 years, smart cards are required in all federal offices. Using a smart card with a government-issued computer has become a standard part of the federal employee's workday. That won't change anytime soon. However, recent history has exposed the limitations of an authentication and access strategy built entirely around traditional smart cards:

- Increasing numbers of remote workers makes issuing and managing traditional smart cards more difficult.
- The EO requires agencies to extend access and authentication protection to government-issued phones and tablets, which are poorly suited to traditional card readers.
- Federal agencies can't adopt a bring-your-own-device (BYOD) strategy because traditional smart cards can't authenticate personal devices prohibited from storing government credentials.
- The future of work is mobile, yet traditional smart cards don't provide the flexibility and accessibility that future calls for or meet the shifting security challenges it will entail.

Replacing smart cards isn't an option. Instead, supplement them with Yubico's security keys, known as YubiKeys, that deliver what traditional smart cards do and much more, building upon existing smart card infrastructure to help make any federal office secure, agile, and fully-compliant.

Business scenarios for YubiKeys

When trying to meet requirements for derived credentials.

When relying more on telework.

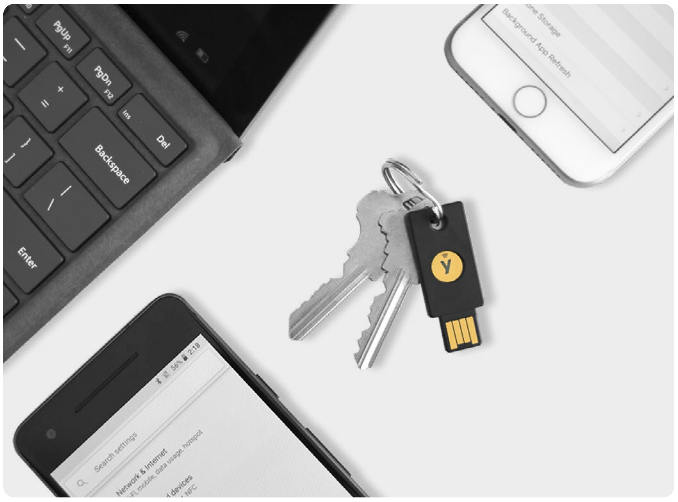
When instituting a BYOD policy.

When building extra security around privileged users like IT admins or high-ranking officials.

When future-proofing an agency for tomorrow's stronger security requirements.

Adding YubiKeys to complement an existing smart card strategy

YubiKeys offer ironclad, hardware-backed authentication protection, require no client software or separate card readers, and are highly ruggedized with no dependence on batteries or cellular connectivity. Employees can just plug their personal YubiKey into any device and touch a button to authenticate themselves and the device. Or can simply tap the YubiKey to an NFC-enabled device for fast authentication. Simple in concept and execution, YubiKeys are a powerful tool for authentication and access – they provide the phishing-resistant MFA required by the EO and are foundational to executing a Zero Trust strategy. More than just a way to get compliant, however, YubiKeys enable modern authentication and access for a new era of government work.



No additional hardware

Save on the cost of purchasing additional hardware such as smart card readers or special laptops with readers, and servers.

Reduced software and management costs

YubiKeys work with the leading Certificate Management Servers (CMS), so agencies can continue to leverage their current CMS investment or migrate to an alternate solution.

Lower IT support burden

Reduce or remove the need for password resets, as well as the high costs associated with password support. Organizations using YubiKeys have been known to reduce support incidents by up to 92%, saving tremendously on IT helpdesk costs, not to mention less user downtime and lost productivity.

With YubiKeys you can give back users valuable time which leads to smoother workflows and higher satisfaction levels. Read about how the New York Air National Guard streamlined operations and the user experience with modern authentication.

Flexible, portable and future-proofed

With a multi-protocol solution that addresses needs for FIDO2/WebAuthn, U2F, OTP, and smart card/PIV, YubiKeys are a future-proofed solution suitable for use across modern and legacy environments, and will support multiple forms of passwordless authentication. Customers who have complex environments can also leverage the YubiKey to enable a bridge to passwordless.

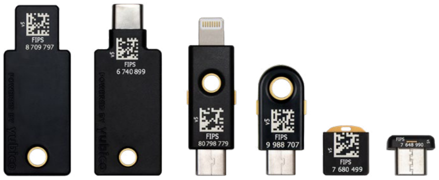
Federally Compliant

The YubiKey meets Federal Government requirements such as FIPS 140-2, NIST SP800-157, and NIST SP800-63-B (AAL3 Credentials). Additionally, the YubiKey enables a derived credential (an alternate secondary credential tied to the PIV/CAC eligibility) for use across multiple devices, government issued or BYOD.

A single solution for modern security, a fast and easy user experience, and compliance

Across the federal government, multiple forces are converging: exploding cyber attacks, the rise of remote work, new security mandates, and greater demands for mobility and accessibility. Each is complicated and important. Unfortunately, many of these forces are in direct opposition—security vs. accessibility, for example.

Balancing the need for security, and an intuitive user experience all while achieving compliance poses major challenges for federal security specialists, with serious consequences for getting it wrong.



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

YubiKeys are the rare solution able to strike that balance while fitting seamlessly into the government's existing smart card program. As a supplement to traditional smart cards, they make authentication easier to manage for a mobile federal workforce eager to use their own devices. And as a solution that enables trusted access, YubiKeys allows for devices and apps off-limits to anyone who has not been verified with a trusted authentication device and process, thereby greatly heightening the security posture for the organization. Finally, as a practical example, Microsoft Azure is now allowing smart cards to be used to log in with a certificate-based authority (CBA), indicating that modern cloud platforms are making it easier to use smart cards in the organizational environment to help enhance the security posture. The YubiKey can handle both Smart Card/PIV and modern FIDO authentication workflows, meeting the organization where it is on the modern authentication journey.

With a single solution, federal agencies can modernize their security infrastructure with a Zero Trust framework, comply with EO #14028 and OMB memo M-22-09 and meet demands for phishing-resistant MFA designed for the way federal employees work today.

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 Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088