Fighting back: How modern security is helping the Federal Government battle rising cyber threats

How Zero Trust and phishing-resistant MFA keep agencies one step ahead

Cyber attacks are on the rise

You don't need a security clearance to know that the U.S. Department of Defense (DOD) and the nation's defense industrial base (DIB) are constant cyberattack targets. In fact, between 2015 and 2022, breaches against the DOD or DIB **more than doubled.**

DOD IT budget that goes towards cybersecurity each year

Source

DOD cyber security budget request for 2023

Source

It's not just the DOD, though

Federal civilian agencies are also under persistent attack. Phishing resistant solutions are critical to protect use cases such as non PIV/CAC eligible employees, contractors, mobile and BYOAD (Bring Your Own Approved Devices), cloud services, air-gapped/isolated networks and citizen-facing digital services.

Government agencies that were compromised in the 2020 SolarWinds hack, including Treasury, Justice, and Energy

Source

The average cost of a public sector cyber attack in 2023, a 25% increase from 2022

Source

> "If there is truly an urgency to innovate within the Defense Department, adopting tools such as YubiKeys should be made a priority to accelerate zero trust security, improve connectivity, and reduce cyber risk across the Joint Force."
>
> **Jeff Burkett**
> Major General, USAF (Ret)
>
> *The quote expressed herein are solely those of the individual and do not necessarily represent the views of the Department of Defense.*

yubico

Unprecedented steps toward winning the war on cybercriminals

In 2021, White House Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," mandated that all US government agencies implement multi-factor authentication (MFA) within 180 days. Shortly thereafter, those requirements got even stronger on both sides.

Department of Defense

The National Security Memorandum NSM-8 on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

Set forth an expectation that the DOD adopt cybersecurity requirements that "are equivalent or exceed" those set forth in the Executive Order

Federal Civilian

OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"

Required that all federal civilian agencies only use phishing-resistant multi-factor authentication

Not all MFA is created equal

Hardware-based security keys such as the YubiKey, is the only technology that complements the PIV and the CAC and provides phishing-resistant MFA for use cases where the PIV and CAC are not suitable or applicable. Below are the benefits of the YubiKey:

- **FIPS 140-2 validated:** Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914)
- **Reduces risk by 99.9%** and stops account takeovers with strongest phishing resistance
- Bridge to modern **FIDO passwordless authentication**
- **Portable root of trust with multiple authentication protocols on a single key:** PIV/CAC, FIDO U2F, FIDO2/ WebAuthn, OTP, OpenPGP

> "The YubiKey will provide our military workforce with a secure tool that provides access to essential information from any device. The simplicity, security, and size makes the YubiKey a valuable component of the mission anywhere and anytime."

Mike Kingsley
Major General, USAF (Ret)

The quote expressed herein are solely those of the individual and do not necessarily represent the views of the Department of Defense.

Discover how to meet these mandates and address emerging use cases in our whitepaper, Modernizing authentication across the Federal Government with phishing-resistant MFA

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries.

For more information, visit: www.yubico.com.

Contact us yubi.co/contact

yubico