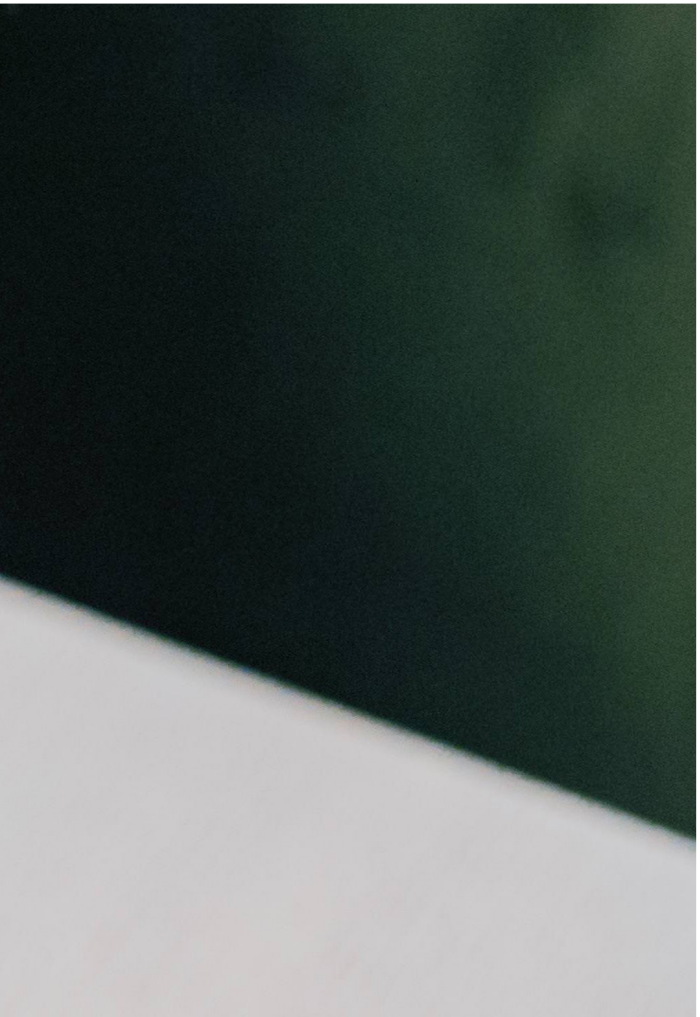
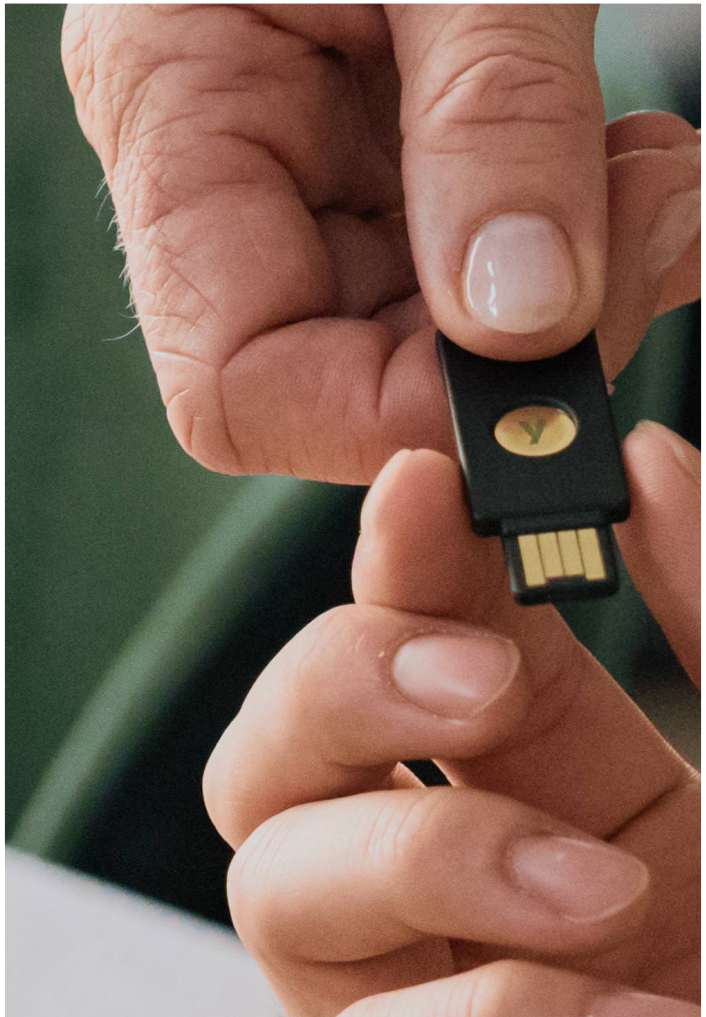
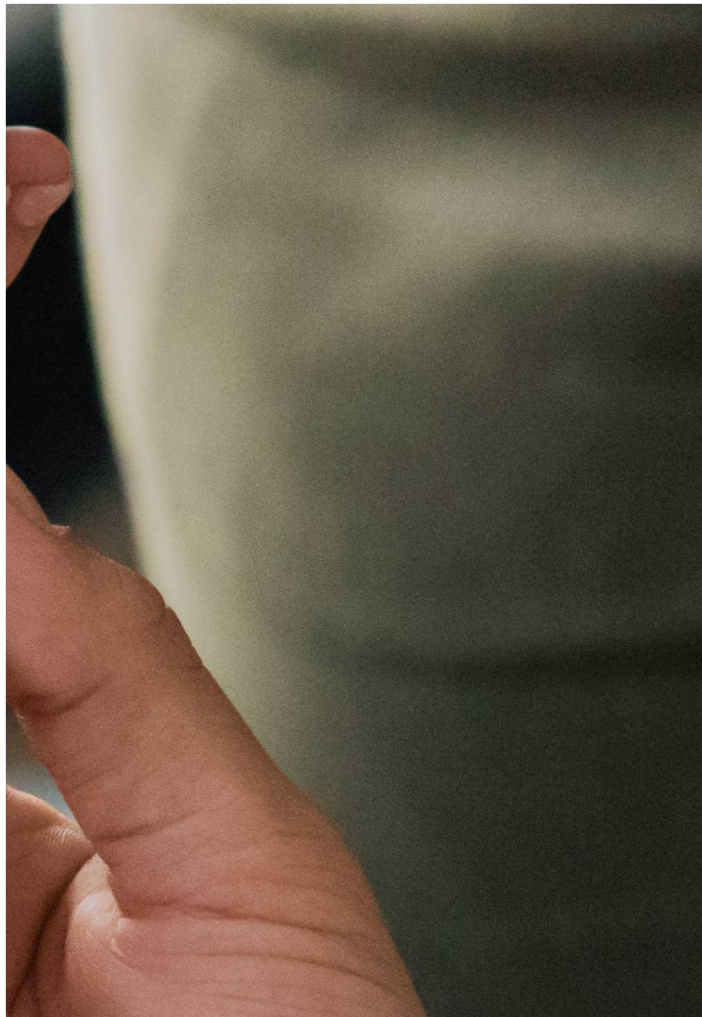
yubico

# Securing Warfighters at the Tactical Edge

Combatant Command Multi-Factor Authentication (MFA) Solution







# Executive Summary

The Department of War (DoW) is strategically shifting away from perimeter-based security toward a comprehensive **Zero Trust Architecture (ZTA)**. This foundational mandate requires **phishing-resistant MFA** to achieve the security, agility, and resilience demanded by the National Defense Strategy. Traditional authentication methods are insufficient to secure the diverse and geographically dispersed networks of U.S. personnel, interagency civilians, and non-CAC eligible partner forces.

**Yubico's FIPS 140-2 validated hardware security keys called YubiKeys** are a DoW-approved solution that directly addresses these converging challenges. The YubiKey is approved by the DoW Chief Information Officer (CIO) as an authenticator that provides hardware-based MFA on DoW networks, supporting both PKI and FIDO2 protocols.

Partnering with Yubico provides a decisive advantage by:

- **Securing Mission Partner Environments:** Delivering unphishable, hardware-based authentication to **non-CAC eligible users** (coalition forces, interagency, host-nation partners), closing a critical security gap. Foreign mission partners are quickly onboarded with secure credentials in order to access mission critical data.
- **Ensuring Mission Assurance at the Tactical Edge:** Providing **ruggedized, power-independent devices** that assure access to data and systems in disconnected, intermittent, and limited (DIL) bandwidth environments.
- **Accelerating Zero Trust and IT Modernization:** Offering a proven, compliant, and scalable solution that meets the **highest Authenticator Assurance Level (AAL3)**.
- **Streamlining Investment and Logistics:** Offering the flexibility of **YubiKey as a Service** for a simple, predictable operational expense (OpEx) model, coupled with secure, direct-to-user logistics via YubiEnterprise Delivery.

# The Strategic Imperative: Zero Trust and Phishing-Resistant MFA

## 1. The Foundation of Zero Trust

Zero Trust (ZT) is the DoW's modern cybersecurity paradigm, based on the principle to **"never trust, always verify"**. This model assumes networks are already compromised and focuses on securing resources directly. A robust Identity, Credential, and Access Management (ICAM) framework is the engine of a Zero Trust architecture.

## 2. Countering Credential Theft

The single greatest threat to any ICAM framework is **phishing**. Adversaries commonly gain access by "logging in" using stolen credentials, having bypassed firewalls and perimeter defenses.

Legacy forms of MFA (e.g., SMS codes, push-based mobile apps) are vulnerable to sophisticated phishing attacks. Consequently, federal and DoW policy mandates the use of **phishing-resistant MFA**. Phishing-resistant authenticators must use **public key cryptography** to create an unphishable transaction and meet the requirements for **NIST SP 800-63B Authenticator Assurance Level 3 (AAL3)**.

The stringent requirement for phishing-resistant MFA is met by only two protocols: **FIDO2/WebAuthn** and **Public Key Infrastructure (PKI)**, both supported by the YubiKey. FIDO2/WebAuthn is the modern, scalable, and user-friendly standard, enabling authentication across diverse platforms and cloud services without the complexity of traditional certificates. PKI, the foundation of the DoW's Common Access Card (CAC), remains essential for securing legacy systems and digital signing. The YubiKey can host multiple PKI credentials and 100 FIDO2 credentials simultaneously, providing the military with unparalleled flexibility. This capability ensures AAL3 compliance for modernizing cloud environments while maintaining necessary compatibility with existing DoD IT infrastructure.

# YubiKey as a Force Multiplier: Tailored Use Cases

The YubiKey 5 FIPS Series is designed to solve the most critical authentication challenges facing Combatant Commands:

| COCOM Challenge | YubiKey Solution/Value Proposition | Supported Credential Types |
|---|---|---|
| **Securing Non-CAC Eligible Partners** (Coalition, Interagency, Foreign Nationals) | Provides FIPS-validated, phishing-resistant MFA as a **DoW-approved authenticator** to enable secure, role-based access for partners. | Local PKI Credentials; FIDO2/ WebAuthn |
| **Assured Access in Austere/Tactical Environments** (DDIL/Air-Gapped) | Keys are **ruggedized (IP68 rated)** and **power-independent**. Cryptographic operations are performed locally, ensuring **offline authentication** and access continuity regardless of network or power. | DoW Mobile PKI Credentials; Local PKI Credentials; FIDO2/WebAuthn |
| **Modernizing IT & Securing Legacy Systems** (Cloud Transition / CAC Augmentation) | Provides **multi-protocol support**, acting as a PIV/CAC-compliant smart card for legacy systems while simultaneously securing new cloud services via modern FIDO2/WebAuthn standards. | DoW Mobile PKI Credentials; Local PKI Credentials; FIDO2/WebAuthn |
| **Protecting High-Value/Privileged Users** (Cyber Operators/Mission Force/Developers and IT Admins) | Immunity to credential theft directly counters the primary attack vector used by sophisticated state actors. Provides a **portable hardware root of trust** that decouples identity from the device. | DoW Mobile PKI Credentials; FIDO2/ WebAuthn |

The YubiKey 5 FIPS Series–from left to right: YubiKey 5C NFC FIPS, YubiKey 5 NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS

YubiKey 5 FIPS Series is currently undergoing FIPS 140-3 validation


YubiHSM 2 FIPS

# Yubico Defense-Ready Product Ecosystem

The **YubiKey 5 FIPS Series** is specifically engineered for U.S. government agencies and provides the highest levels of security and compliance.

- **FIPS 140-2 Validation:** The series meets the FIPS 140-2 requirements (Overall Level 2, Physical Level 3), certifying it for the highest assurance level (AAL3) for digital identity. YubiKey 5 FIPS Series is currently undergoing FIPS 140-3 validation.
- **Secure Supply Chain:** FIPS YubiKeys are securely manufactured in the **United States**, mitigating supply chain risks critical for DoW deployment.
- **Multi-Protocol Support:** A single YubiKey supports FIDO2, WebAuthn, Smart Card (PIV-compatible), Yubico OTP, and OATH-TOTP/HOTP.
- **Diverse Form Factors:** USB-A, USB-C, Lightning, and NFC to support every device and use case, from headquarters workstations to tactical mobile devices.

| Product Name | Form Factor / Connectors | Ideal Use Case Examples (Generic) |
|---|---|---|
| YubiKey 5 NFC FIPS | Keychain / USB-A, NFC | Standard issue for personnel, compatible with legacy desktops and NFC-enabled mobile devices. |
| YubiKey 5C NFC FIPS | Keychain / USB-C, NFC | Issued for modern laptops and Android devices. |
| YubiKey 5Ci FIPS | Keychain / USB-C, Lightning | For staff using iPhones and iPads for secure mobile C2. |
| YubiKey 5C Nano FIPS | Nano / USB-C | “Set and forget” for use in ruggedized laptops and tactical equipment. |

For securing backend systems and the root of trust, Yubico also offers the **YubiHSM 2 FIPS**, a FIPS 140-2 validated hardware security module ideal for protecting cryptographic keys for Certificate Authorities, database encryption, and code signing, including in Commercial Solutions for Classified (CSfC) capabilities at the tactical edge

# Implementation and Procurement Pathways

Integrating Yubico's capabilities, including the YubiKey as a Service offering, can be achieved through a phased, scalable strategy, leveraging streamlined DoW procurement vehicles.

## YubiKey as a Service: A Predictable, Future-Ready Investment

For enterprise-wide adoption, the Command should consider the financial and logistical power of **YubiKey as a Service**. This innovative solution transforms the procurement of phishing-resistant hardware keys from a complex capital expenditure (CapEx) to a predictable operational expense (OpEx) model.

- **Budget Certainty:** Lock in simple, annual per-user pricing, eliminating the financial uncertainty of large, one-time hardware purchases and ensuring continuous budget alignment. This ensures you maintain AAL3 compliance without unexpected procurement hurdles.
- **Always Current, Always Compliant:** YubiKey as a Service includes an automatic key refresh, guaranteeing your Zero Trust architecture always leverages the latest FIPS-validated technology and the most current security innovations without requiring separate procurement cycles.
- **Simplified Logistics (YubiEnterprise Delivery):** YubiKey as a Service is seamlessly paired with YubiEnterprise Delivery, providing secure, direct-to-user shipping globally. This minimizes administrative overhead, eliminates the need for large-scale inventory management, and rapidly equips your diverse force, from HQ to the tactical edge, ensuring mission continuity.

## Phased Implementation Strategy (“Crawl-Walk-Run”)

1. **Crawl (Pilot Program):** Initiate a focused pilot program to equip a deployed task force or participants of a major multinational exercise with YubiKeys. This phase validates the ease of provisioning, security benefits, and operational workflow in an operational environment.

2. **Walk (Expanded Rollout):** Expand the rollout to address the high-priority security gap of all **non-CAC eligible personnel** requiring access to command networks, including partners, contractors, and interagency staff.

3. **Run (Enterprise Adoption):** Integrate YubiKeys as a standard authenticator across the entire enterprise, making it a primary authenticator for mobile, partner-nation, and tactical edge use cases, solidifying a key component of the command’s Zero Trust roadmap.workstations, including Chromebooks and personal phones. When a YubiKey has been provisioned with DoD Purebred credentials, it becomes a portable root of trust for service members’ identities, making it easier to authenticate regardless of the device. Streamlined DoW and Government Procurement.

## Streamlined DoW and Government Procurement

Yubico solutions are readily available through multiple established DoW and government-wide contract vehicles, simplifying acquisition.

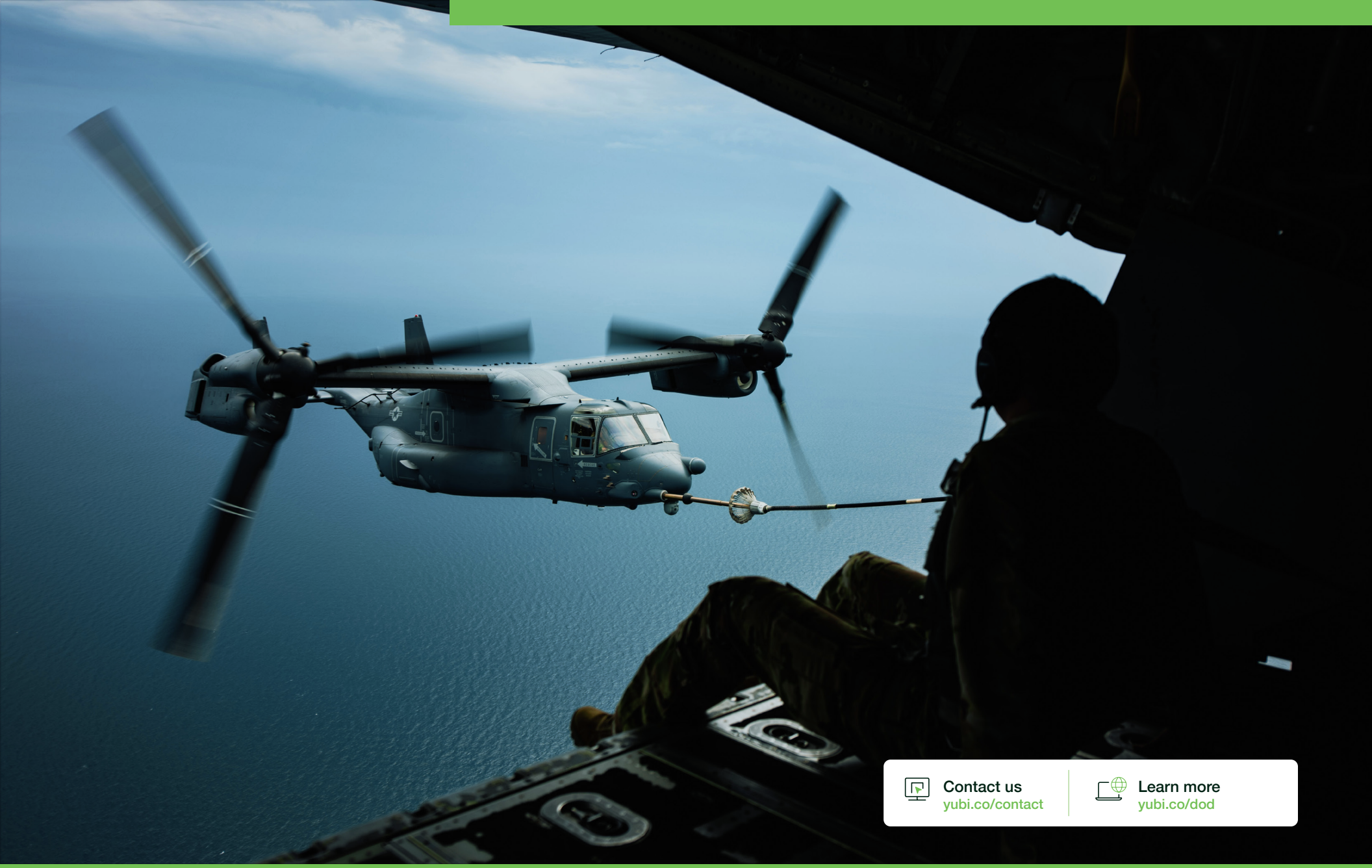
Adopting Yubico’s FIPS-validated authentication solutions is a critical and immediate step the Combatant Command can take to secure its forces, protect its mission, and maintain a decisive advantage in today’s contested global environment.

# References:

**U.S. Department of Defense.** (2025, October 24). Multi-Factor Authentication (MFA) for Unclassified & Secret DoD Networks (Memorandum). (Signed by Katherine Arrington, Performing the Duties of the Chief Information Officer of the Department of Defense).

**U.S. Department of Defense, Chief Information Officer.** (2019, December 20). DoD Mobile Public Key Infrastructure (PKI) Credentials (Memorandum). (Signed by Dana Deasy, Chief Information Officer of the Department of Defense).

**U.S. Department of Defense, Chief Information Officer.** (2017, April 14). Approval of Multi-Factor Authentication Alternatives – Rivest Shamir and Adleman and YubiKey (Memorandum). (Signed by Essye B. Miller, Deputy Chief Information Officer for Cybersecurity and DoD Senior Information Security Officer).



**Contact us**
yubi.co/contact

**Learn more**
yubi.co/dod

yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: **www.yubico.com.**