yubico

HOW THE YUBIKEY SOLVES DIB USE CASES WITH PHISHING-RESISTANT MFA

Protecting the supply chain across the Defense Industrial Base with modern authentication

The urgency to harden cybersecurity defenses across the Defense Industrial Base

79%

of DOD contractors lack comprehensive MFA

Source

72%

of the top 100 defense contractors leaked at least one credential in a 90 day span

Source

$2.55 billion USD

The average cost of a public sector cyber attack in 2024

Source

Increasing threats and tightening security controls

Industries such as the Defense Industrial Base (DIB) manufacturing sector are a prime target for cyberattacks. Stolen credentials gained through phishing or weak, legacy authentication processes pose as entry points for threat actors. Today's attackers don't hack in, they just log in.

Despite barriers to change such as legacy infrastructure, complex industrial and restrictive production floor environments, and the high cost of operational disruption, the DIB faces an imperative to move beyond passwords to modern authentication solutions.

Government contractors are required to implement mandatory controls for Controlled and Unclassified Information (CUI) detailed by National Institute of Standards and Technology (NIST) SP 800-171.The draft NIST SP 800-171 r3 will require a shift to multi-factor authentication (MFA), specifically phishing resistant authentication (aka replay-resistant authentication), for access to system accounts—not just for privileged accounts. In fact, the most recent self-assessment methodology reflects a deduction in scoring if MFA is implemented only for remote and privileged users rather than all users and adds an additional point if MFA is phishing-resistant. The Cybersecurity Maturity Model Certification (CMMC) 2.0 is the Department of Defense's (DoD) unified standard of certification and attestation requirements for implementing cybersecurity across the defense industrial base, consisting of 14 domains and three maturity levels that align to NIST standards.

CMMC Model 2.0

In order to ensure the safety of intellectual property (IP), weapon systems and to protect operational capabilities, sensitive information, product integrity and national security, the DIB needs to ensure robust cyber security measures are deployed, including but not limited to—protecting identities, data and systems, with the most modern, secure solutions available today.

Level 3 Expert	**Level 2** Advanced	**Level 1** Foundational
Model 110+ practices based on NIST SP 800-171 and 800-172 **Assessment** Triennial government-led assessments	**Model** 110+ practices aligned with NIST SP 800-171 **Assessment** Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs	**Model** 15 practices **Assessment** Annual self-assessment & annual affirmation

On March 12, 2024, revisions to 32 CFR § 236, "Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Activities" were published in the Federal Register as a Final Rule, to be made effective April 11, 2024. The Final Rule expands eligibility for the DIB CS Program from only contractors that possess an active Facility Clearance to all defense contractors who own or operate an unclassified information system that processes, stores, or transmits Controlled Unclassified Information (CUI).

Read more here

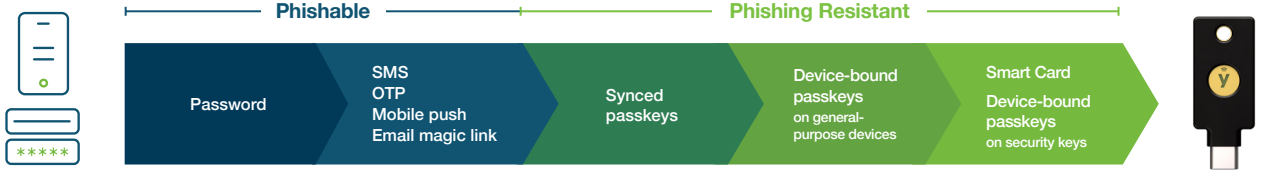
Defense Industrial Base (DIB) Guide to Implementing the Cybersecurity Framework

Modernizing existing information technology (IT) and operational technology (OT) systems is challenging and complex. Barriers to change include legacy technology that often does not support modern security controls, diverse industrial and restrictive production floor environments, over reliance on local and traditional on-prem access compared to the cloud, third-party remote connections to control OT devices connected to an internal network becoming more difficult to manage, and a shift in mindset from risk awareness and risk tolerance to one of proactivity.[3] All of these factors lead to competing business priorities and combine to create greater difficulty in achieving a more technologically modern state.

Not all MFA is created equal

Multi-factor authentication (MFA) should be a first-line defense of any cybersecurity strategy to protect critical data, IT and OT environments.. And while any MFA is better than passwords, not all forms of MFA offer the same level of security or frictionless user experience. Legacy forms of MFA such as short message service (SMS), one-time password (OTP) and push notification apps are highly susceptible to modern day phishing attacks. To stay ahead of evolving cyber threats including AI-driven phishing attacks, it is essential to protect sensitive and critical data and infrastructure with modern phishing-resistant MFA.

What is phishing-resistant MFA? Phishing-resistant MFA processes rely on cryptographic verification directly between devices or between the device and a domain, making them highly secured against attempts to compromise or subvert the authentication process. A minimum standard met only by PIV/Smart Card and MFA based upon the FIDO2/WebAuthn standard.



Protecting all users in the enterprise

Start by addressing key user populations. Expands to broader set of stakeholders.

Privileged access
Secure priviledged account users

Mobile restricted
Secure call centers for mobile restricted users

Shared workstations
Protect shared workstation users

Remote workforce
Enable remote workforce

Office workers
Improved UX and security for office workers

3rd party access
Protect corporate system access by 3rd parties

End customers
Safeguard your end customers

Safeguard DIB IT and OT ecosystem with Yubico phishing-resistant solutions

Yubico solutions meet you where you are on your cybersecurity journey, while paving the way to a modern, phishing-resistant authentication infrastructure, and jumpstarting your plans to implement a zero trust framework. With Yubico solutions, you can be confident that your data and intellectual property are secured, and product integrity is always ensured.

The YubiKey

A pioneer in modern, hardware-based authentication and Yubico's flagship product, the YubiKey is designed to meet you where you are on your authentication journey by supporting a broad range of authentication protocols, including FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart Card/PIV.

yubi.co/key

Yubico Hardware Security Module (HSM)

The world's smallest HSM, YubiHSM 2, packs a lot of power, and offers game changing cryptographic protection for servers, applications and computing devices. Secure your public key infrastructure (PKI) environments, encrypt your files and databases and securely sign code or any digital artifact to raise the bar for security for your OT and IT systems.

yubi.co/hsm

YubiKeys as a Service

Get peace of mind in an uncertain world with a YubiKey subscription service that makes supporting new hires, tackling employee turnover and securing remote/hybrid workers fast, flexible and future-proofed—all with a lower cost to entry.

This service provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits.

yubi.co/subscription

YubiEnterprise Delivery

Accelerate your journey to phishing-resistant MFA with an end-to-end domestic and international YubiKey delivery service. Let Yubico and our global partners worry about the logistics so you can focus on bigger business issues.

yubi.co/delivery

Manufacturing clean floor and sterile environments

Authentication is a mission-critical service. If employees can't log into apps or portals they use, they can't do their jobs. How do you secure shared terminals and devices with multiple rotating users commonly found across the manufacturing clean floors and similar sterile environments, making sure both the user accounts are secure and that the users are gaining access to only the applications, services and data they should have access to? Further, it is important in a manufacturing context to ensure that the authentication solution does not introduce new security or safety challenges.

The YubiKey doesn't just provide strong authentication—it is also highly portable and easy to use. A single security key works across multiple devices such as desktops, laptops, mobile, tablets, and notebooks without requiring a battery or internet connection. Users can authenticate with a simple touch or tap—using NFC capability with a wearable, which provides the easiest and most secure experience possible. This is especially critical in clean floor and sterile environments, where mobile phones are not allowed. YubiKeys are also crush resistant, and IP68 certified, as well as dust and water-resistant.

The YubiKey can be used to ensure secure, phishing-resistant authentication for remote users performing mission-critical functions that would otherwise require in-person presence. With today's international workforces, organizations must utilize the most secure communications channels and phishing-resistant solutions available to ensure only authorized users are allowed access to confidential data, systems, and virtual manufacturing floors.

Secure augmented reality access

Augmented reality is becoming increasingly common to support DoD medical and virtual medical training, virtual combat training, maintenance, flight simulations and more. For the defense sector, security is vital, and solutions that run on Head Mounted Devices (HMD) or that support spatial computing with multiple cameras, sensors, and connectivity to the network, can pose a cybersecurity or related risk unless proper security is ensured for both data at rest and data in transit.

Corporate access across secure spaces

Many corporate users may be required to securely access corporate resources across secure spaces such as SCIFs, on a base, overseas, and from other secure locations. The multi-protocol capability of YubiKeys ensures phishing-resistant MFA options that work well in secure spaces, isolated networks and mobile restricted environments as YubiKeys don't need any network connectivity, cellular connection, or batteries to work. YubiKeys are also compatible with Cross Domain Solution (CDS) and Multi-Level Security (MLS), and users can be authenticated across secure spaces without any transfer of information.

Secure supply chain

Supply chains include not just a mix of third party physical goods and components used to manufacture products, but also rely on third-party code used to build the product and for the business to function smoothly. Securing the supply chain requires securing both user access and any inputs (physical component, software, or data) to the manufacturing process, to ensure quality and integrity of the product, protection against stolen intellectual property (IP), or lost production time.

The primary challenge for the DIB is that protecting downstream sub-contractor supply chains is not easy given the hundreds (if not thousands) of entry points that need to be monitored along the way. DIBs must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain.

DIB prime contractors can use YubiKeys to provide modern phishing-resistant authentication at scale across the end-to-end supply chain. YubiKeys provide suppliers, subcontractors, or any user who has upstream access to the network or during critical IP handoffs, with phishing-resistant and easy-to-use authentication.

The YubiHSM 2 enables secure, tamper-resistant key storage and operations by preventing accidental copying and distribution of cryptographic keys, and preventing remote theft of keys stored in software. Since the YubiHSM 2 is designed to store cryptographic keys, it is ideally suited to protect PKI infrastructure and its network of cryptographic keys, enabling the DIB to verify the authenticity of each component being manufactured.

Ensuring the highest integrity of your product parts

The DIB knows it is crucial to ensure that all components involved in an end-to-end process are authentic to avoid unsolicited replication and theft, but also for quality assurance, since an assembly line should only consist of genuinely sourced products. As a result, there must always be a solution in place to protect the integrity and intellectual property of all components from production and assembly, to repair and replacement.

The traditional approach to protect intellectual property (IP) and prevent counterfeiting in manufacturing involves the use of digital cryptographic keys and encryption. Cryptographic keys would be stored either in software, which is highly vulnerable, or a hardware security module (HSM). Unfortunately, traditional rack-mounted and cardbased HSMs are large and expensive, making them impractical on the assembly floor, in caged data centers, or for IoT devices.

Mitigrating data protection compliance risk in manufacturing

Every business has personal data that is subject to stringent data privacy and cybersecurity laws and regulations. Further, many manufacturers must become ISO certified or adhere to higher standards to meet contractual requirements—particularly in the Federal space. The YubiKey and YubiHSM 2 can help manufacturers comply with required and voluntary data security standards. This checklist will help you frame how Yubico products easily satisfy compliance requirements:

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

The YubiHSM Series—from left to right: YubiHSM 2, YubiHSM 2 FIPS

EO 14028 on Improving the Nation's Cybersecurity / OMB Memo M-22-09

Implement phishing-resistant MFA

CMMC 2.0 / DFARS Defense Federal Acquisition Regulation Supplement

Attest to practices aligned with NIST SP 800-171

CISA and NSA Best Practices in Identity and Access Management

Implement phishing-resistant MFA

National Institute of Standards and Technology (NIST) SP 800-63-3 / 4 Digital Identity Guidelines

Meets Authenticator Assurance Level 3 (AAL3) for hardware-based authenticator

Meets revised definition for phishing-resistance

ISO/IEC 27001 standard for Information Security Management System (ISMS)

Annex A.9 Safeguard access to information

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

3.5.2 Authenticate the identities of users, processes or devices before allowing access to organizational systems

3.5.3 MFA for local and network access to privileged accounts and for network access to non-privileged accounts

IEC 62443 Security for Industrial Automation and Control Systems

262 Verify third-party components

264 Reliably identify and authenticate all users

The path forward to phishing-resistant MFA at scale

No matter where you are on your MFA journey, we'll meet you there. You can accelerate your zero trust approach and gain a bridge to a passwordless future. With a tried and true process that hundreds of organizations have followed already—and with a 'YubiKey as a Service' model—it's not a matter of if you'll be successful but when you'll be successful in raising your bar for security with modern, hardware-based security keys.

A worthwhile investment that not only shows that you care about the safety of employee authentication experiences, and cybersecurity across your supply chain, but will drive competitive differentiation and bolster you as a thought leader.

Plan

Ensure readiness by clarifying use cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

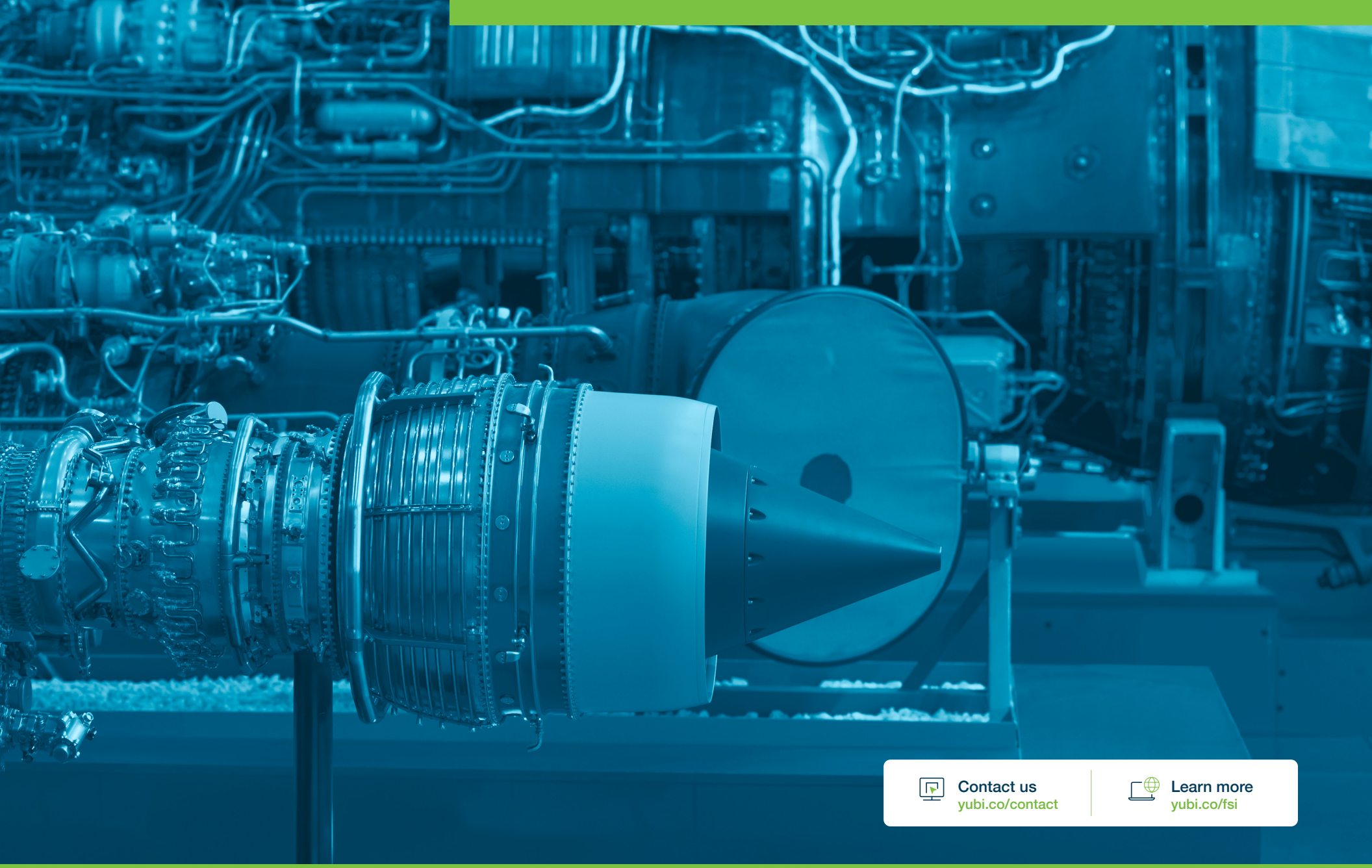
Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact



Contact us
yubi.co/contact

Learn more
yubi.co/fsi

yubico
The key to trust

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, please visit: **www.yubico.com.**