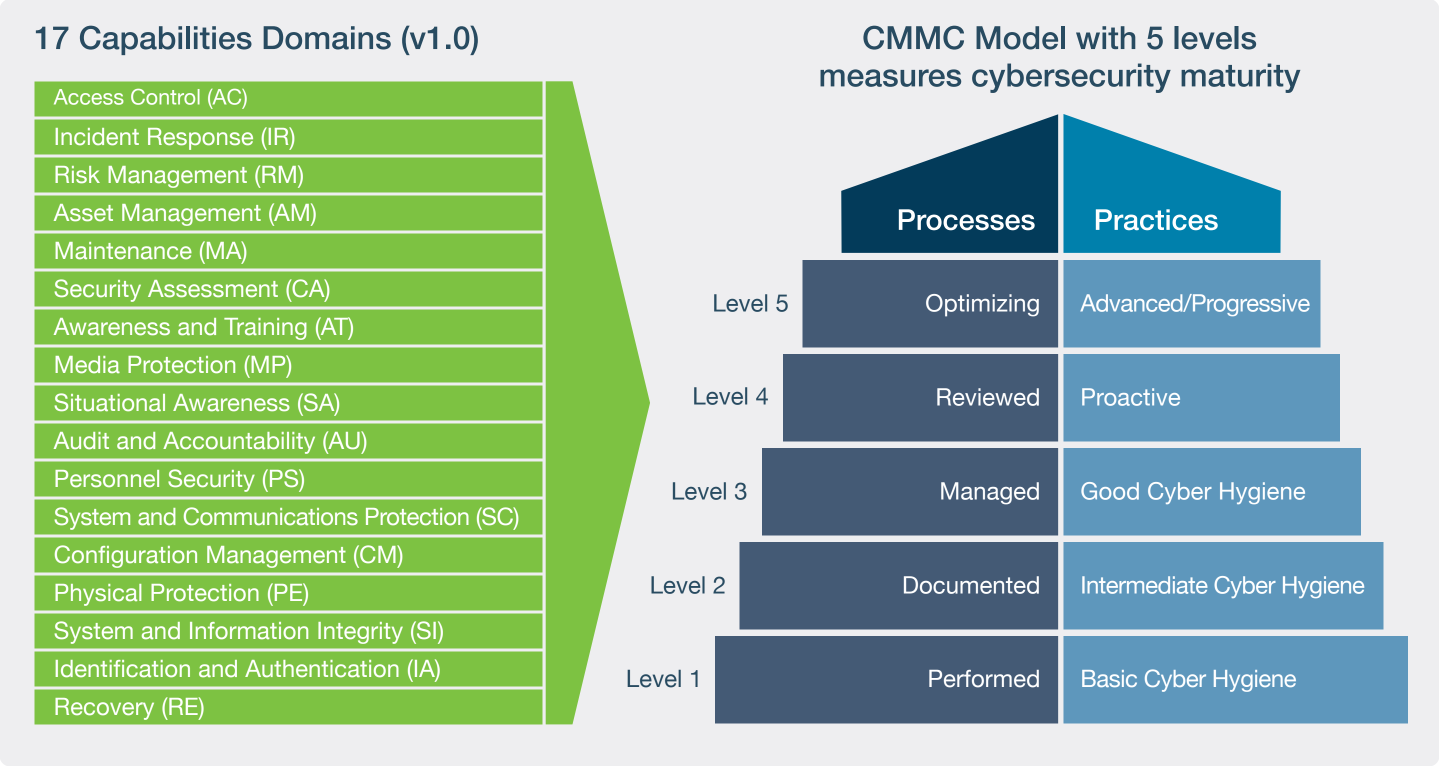
How the YubiKey Helps Department of Defense Contractors Meet the Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's (DoD) unified standard for implementing cybersecurity across the defense industrial base, consisting of 17 domains and five maturity levels. This document addresses the specific CMMC domains and capabilities that the YubiKey meets or exceeds pertaining to the following domains—Identification and Authentication, Access Control, Asset Management, Audit and Accountability, Maintenance, and Media Protection.



17 Capabilities Domains (v1.0)

- Access Control (AC)
- Incident Response (IR)
- Risk Management (RM)
- Asset Management (AM)
- Maintenance (MA)
- Security Assessment (CA)
- Awareness and Training (AT)
- Media Protection (MP)
- Situational Awareness (SA)
- Audit and Accountability (AU)
- Personnel Security (PS)
- System and Communications Protection (SC)
- Configuration Management (CM)
- Physical Protection (PE)
- System and Information Integrity (SI)
- Identification and Authentication (IA)
- Recovery (RE)

CMMC Model with 5 levels measures cybersecurity maturity

	Processes	Practices
Level 5	Optimizing	Advanced/Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

The CMMC domain—Identification and Authentication (IA.3.083) in particular lists the requirement for multi-factor authentication. The YubiKey, a hardware security key that is designed to stop account takeovers, meets this level III requirement by providing highest-assurance multi-factor authentication through a number of protocols for local and network access. YubiKeys support multiple authentication protocols including smart card PIV/CAC, FIDO U2F, FIDO2 and OTP (HOTP, TOTP, YubiOTP). Specific to smart card PIV/CAC, a user is required to enter a PIN to unlock the secure element on the YubiKey as one factor, and the second factor is the possession of the private key securely stored on the YubiKey, which is used in the authentication workflow. The YubiKey can also be used in conjunction with passwords or PIN to provide multi-factor authentication leveraging the FIDO U2F, FIDO2 and OTP (HOTP, TOTP, YubiOTP) protocols.

- A Department of Defense (DoD) Privileged User Working Group (PUWG) and Deputy CIO for Cybersecurity (DCIO-CS) Memo released August 20th, 2018 approved YubiKeys for use as a multi-factor authentication (MFA) token for DoD unclassified and secret classified information systems and applications.
- The YubiKey is the only FIPS-validated security key (Certificate #3517 Overall Level 2, Physical Security Level 3) that is made in the USA, complies with the Trade Agreements Act (TAA), and meets the most stringent secure supply chain requirements.

The tables below showcase how the YubiKey helps DoD contractors and/or their sub-contractors meet CMMC for Identification and Authentication, Access Control, Asset Management, Audit and Accountability, Maintenance, and Media Protection domains.

Domain: Access Control (AC)

CMMC Capability	CMMC Level	YubiKey Benefits
C001 Establish system access requirements	**Level 1** **AC.1.001** **Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).** • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 1 3.1.1 • CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 • AU ACSC Essential Eight	Access can be controlled and limited by the YubiKey leveraging the PIV/CAC module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled.
C002 Control internal system access	**Level 1** **AC.1.002** **Limit information system access to the types of transactions and functions that authorized users are permitted to execute.** • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 **Level 2** **AC.2.007** **Employ the principle of least privilege, including for specific security functions and privileged accounts.** • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5) • UK NCSC Cyber Essentials	YubiKeys can meet up to Level 3 maturity control by providing strong hardware backed access controls; controlling and limiting access with the YubiKey via the PIV/CAC module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled. AC.3.019 - Terminate (automatically) user sessions after a defined condition. A smart card policy can be implemented in such a way that when the YubiKey is removed from the computer, the OS is locked.

(continued on next page)

	AC.2.008 **Use non-privileged accounts or roles when accessing nonsecurity functions.** • NIST SP 800-171 Rev 1 3.1.6 • CIS Controls v7.1 4.3, 4.6 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-6(2) • UK NCSC Cyber Essentials Level 3 AC.3.018 **Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.** • NIST SP 800-171 Rev 1 3.1.7 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6(9), AC-6(10) AC.3.019 **Terminate (automatically) user sessions after a defined condition.** • NIST SP 800-171 Rev 1 3.1.11 • CIS Controls v7.1 16.7, 16.11 • NIST SP 800-53 Rev 4 AC-12	

Domain: Asset Management (AM)		
CMMC Capability	CMMC Level	YubiKey Benefits
C006 Manage asset inventory	Level 4 AM.4.226 **Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.** • CMMC modification of Draft NIST SP 800-171B 3.4.3e • CIS Controls v7.1 1.1, 1.2, 1.4, 1.5, 2.3, 2.4, 2.5 • NIST CSF v1.1 ID.AM-1, ID.AM-2 • CERT RMM v1.2 ADM:SG1.SP1 • NIST SP 800-53 Rev 4 CM-8	Leveraging a certificate management system (CMS), YubiKey's can be managed as an asset. Additionally, the firmware information can be retrieved and stored as well.

Domain: Audit and Accountability (AU)

CMMC Capability	CMMC Level	YubiKey Benefits
C009 Identify and protect audit information	**Level 2** **AU.3.049** **Protect audit information and audit logging tools from unauthorized access, modification, and deletion.** • NIST SP 800-171 Rev 1 3.3.8 • CERT RMM v1.2 MON:SG2.SP3 • NIST SP 800-53 Rev 4 AU-6(7), AU-9 **AU.3.050** **Limit management of audit logging functionality to a subset of privileged users.** • NIST SP 800-171 Rev 1 3.3.9 • CERT RMM v1.2 MON:SG2.SP2 • NIST SP 800-53 Rev 4 AU-6(7), AU-9(4)	Access can be controlled and limited by the YubiKey leveraging the PIV/CAC module. Using the YubiKey as a smart card, authorization policies are centralized and access is tightly controlled.

Domain: Identification and Authentication (IA)

CMMC Capability	CMMC Level	YubiKey Benefits
C015 Grant access to authenticated entities	**Level 3** **IA.3.083** **Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.** • NIST SP 800-171 Rev 1 3.5.3 • CIS Controls v7.1 4.5, 11.5, 12.11 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 IA-2(1), IA-2(2), IA-2(3) • AU ACSC Essential Eight **IA.3.084** **Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts** • NIST SP 800-171 Rev 1 3.5.4 • NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7 • NIST SP 800-53 Rev 4 IA-2(8), IA-2(9)	The YubiKey can provide multi-factor authentication through a number of protocols for local and network access. By default, PIV/CAC and FIDO2 based authentication provide multi-factor authentication by having the user enter a PIN to unlock the secure element on the YubiKey as one factor (something you know). The second factor would be the possession of the private key that is used in the authentication ceremony. The private key does not leave the YubiKey (something you have). The YubiKey can also be used in conjunction with passwords or PIN to provide multi-factor authentication leveraging FIDO U2F, FIDO2 or OTP (HOTP, TOTP, YubiOTP) based protocols. IA.3.084 YubiKeys are resistant to replay attacks by leveraging standards that take this into account. PIV/CAC and FIDO2 required possession of the physical YubiKey. OTP based protocols are time or hash based synchronous.

Domain: Maintenance (MA)

CMMC Capability	CMMC Level	YubiKey Benefits
C021 Manage maintenance	**Level 2** **MA.2.113** **Require multi-factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.** • NIST SP 800-171 Rev 1 3.7.5 • NIST CSF v1.1 PR.MA-2 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 MA-4	The YubiKey can provide multi-factor authentication through a number of protocols for local and network access. By default, PIV/CAC and FIDO2 based authentication provide multifactor authentication by having the user enter a PIN to unlock the secure element on the YubiKey as one factor (something you know). The second factor would be the possession of the private key that is used in the authentication ceremony. The private key does not leave the YubiKey (something you have). The YubiKey can also be used in conjunction with passwords or PIN to provide multifactor authentication leveraging FIDO U2F, FIDO2 or OTP (HOTP, TOTP, YubiOTP) based protocols. Given the portability and standard form factors, YubiKey's can easily be given to third parties that perform remote access to internal systems.

Domain: Media Protection (MP)

CMMC Capability	CMMC Level	YubiKey Benefits
C023 Protect and control media	**Level 3** **MP.3.123** **Prohibit the use of portable storage devices when such devices have no identifiable owner.** • NIST SP 800-171 Rev 1 3.8.8 • NIST CSF v1.1 PR.PT-2 • CERT RMM v1.2 MON:SG2.SP4 • NIST SP 800-53 Rev 4 MP-7(1)	Even though the YubiKey may interface with the computer via a USB port, it is not a portable storage device. It does not have the capacity to store media.

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

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