Multifactor Authentication for the CMMC Environment

Controls, Conflicts, and Implementation Realities

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

Introduction

CMMC Level 2 requires multifactor authentication for all network access to systems that process, store, or transmit Controlled Unclassified Information. The requirement traces directly to NIST SP 800-171 Revision 2, control 3.5.3 (IA.L2-3.5.3), which states that organizations must use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. Organizations relying on password-only authentication will not satisfy this control, and in practice, assessors treat MFA as a prerequisite for certification rather than a deficiency that can be deferred.

The principle is straightforward: a password alone is not sufficient. Authentication must combine at least two distinct factors drawn from three categories. Something you know, such as a password or PIN. Something you have, such as a hardware token or smart card. Something you are, such as a fingerprint or other biometric characteristic.

In practice, however, MFA implementation introduces a series of decisions that intersect with other CMMC controls in ways that many contractors do not anticipate. The choice of authenticator type affects media protection policy, mobile device management, USB port configuration, and audit logging requirements. An organization that selects its MFA solution in isolation from these adjacent controls risks creating a configuration that satisfies one requirement while failing another.

This paper is intended for IT leadership and compliance staff at small and mid-size Defense Industrial Base contractors. It examines the MFA requirement in the context of the full CMMC Level 2 control set, identifies the implementation conflicts that contractors will encounter, evaluates the major authenticator options against both compliance and operational criteria, and provides practical guidance for selecting and deploying an MFA approach that will withstand assessment scrutiny. The paper also includes a sample System Security Plan entry for IA.L2-3.5.3 and addresses the limitations on deferring MFA through a Plan of Action and Milestones.

The Control Requirement

IA.L2-3.5.3 is the primary MFA control within CMMC Level 2. It requires multifactor authentication for two distinct access scenarios: local and network access to privileged accounts, and network access to non-privileged accounts. This means that every user accessing CUI-scoped systems over the network must authenticate with at least two factors, regardless of their privilege level.

The control does not specify which authenticator types are acceptable. That guidance comes from NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, which defines authenticator assurance levels and classifies specific authenticator types. While CMMC does not formally mandate a specific assurance level or require compliance with 800-63B, assessors commonly reference its principles when evaluating whether an MFA implementation is adequate. Organizations should treat 800-63B as an informative reference that shapes assessment expectations.

Organizations relying on password-only authentication are not meeting IA.L2-3.5.3. Under current assessment practice, this is not a control that lends itself to a Plan of Action and Milestones as a path to certification. Assessors will test MFA directly during the assessment by observing login procedures, reviewing system configurations, and verifying that single-factor access paths do not exist within the assessment scope.

The Three Authentication Factors

Multifactor authentication requires the combination of at least two factors from the following three categories. Understanding these categories is essential because CMMC assessors will verify that the factors in use are genuinely distinct and not two instances of the same category.

Something You Know. This factor relies on information the user has memorized or can recall, such as a password, PIN, or security question response. It is the most common baseline factor and is present in nearly every MFA deployment as the first element of the authentication pair.

Something You Have. This factor requires a physical object in the user's possession. Examples include a hardware security key (such as a YubiKey or Feitian device), a PIV or CAC smart card, a hardware OTP token (such as an RSA SecurID), or a registered mobile device running an authenticator application. Possession-based factors are the most common second factor in enterprise MFA deployments.

Something You Are. This factor uses a biometric characteristic of the user, such as a fingerprint, facial recognition, retinal scan, or voice pattern. Biometric factors are increasingly available on modern endpoints, but they introduce additional considerations that the following paragraphs address.

The most common MFA deployment combines a password with a possession-based factor such as a hardware key or authenticator application. Biometric factors are less commonly deployed as the primary second factor, and organizations considering them should understand the additional complexity involved.

Biometric authentication requires an enrollment process in which each user's biometric template is captured and stored. Organizations must determine where those templates are stored (on the device, on a server, or within a hardware security module), how they are protected, and what policies govern their retention and deletion. Biometric data is inherently sensitive and, unlike a password or a hardware key, cannot be revoked or reissued if compromised. Organizations must also define fallback authentication procedures for situations where biometric verification fails, such as sensor malfunction, physical injury, or environmental conditions that affect sensor accuracy. This is particularly relevant for contractors operating in manufacturing, machine shop, or shop-floor environments, where gloves, debris, temperature extremes, and high employee turnover can cause frequent sensor failures and complicate enrollment logistics. For these reasons, biometric factors are best suited as a supplemental layer within a broader MFA architecture rather than as the sole second factor.

Acceptable MFA Methods for CMMC Environments

Not all MFA methods carry the same level of assurance or the same level of risk. The following analysis evaluates common authenticator types against both the NIST guidance and the practical realities of CMMC assessment.

FIDO2 and U2F Hardware Security Keys

FIDO2-compliant hardware security keys, such as the YubiKey series and Feitian ePass devices, represent the strongest generally available authenticator for CMMC environments. These devices use public key cryptography to bind authentication to the specific relying party, which makes them resistant to phishing, man-in-the-middle attacks, and credential replay. The authenticator generates a unique key pair for each service, and the private key never leaves the device.

FIDO2 keys connect via USB, NFC, or Bluetooth. They qualify as something you have, and when combined with a password (something you know), they satisfy the two-factor requirement. Organizations deploying FIDO2 keys should provision at least two keys per user to ensure continuity if a primary key is lost or damaged.

Organizations seeking the highest level of cryptographic assurance should select FIDO2 keys that carry FIPS 140-2 or FIPS 140-3 validation. The YubiKey 5 FIPS Series is one example of a commercially available FIDO2 key with FIPS 140-2 validation at Level 2. While CMMC Level 2 does not explicitly mandate FIPS-validated authenticators, selecting validated hardware strengthens the organization's posture for future requirements, including potential alignment with Zero Trust architectures and any future CMMC Level 3 expectations.

From an assessment perspective, FIDO2 keys produce clear, auditable evidence. The identity provider logs will show that authentication required the hardware key, and the key itself cannot be cloned or transferred to another device.

PIV and CAC Smart Cards

Personal Identity Verification (PIV) cards and Common Access Cards (CAC) are the federal standard for strong authentication. PIV cards contain a cryptographic certificate issued by a trusted Certificate Authority and require a PIN to unlock, which means a single PIV card provides two factors in one device: something you have (the card) and something you know (the PIN).

For contractors already participating in federal programs that issue CAC or PIV credentials, leveraging those credentials for CMMC-scoped system access is a natural and defensible approach. NIST SP 800-157 provides guidance on PIV-derived credentials for environments where the physical card reader infrastructure is impractical.

Hardware OTP Tokens

Hardware one-time password tokens, such as the RSA SecurID, generate a time-based or event-based code that the user enters alongside a password. These devices have a long track record in enterprise environments and are well understood by assessors.

Hardware OTP tokens are something you have. Combined with a password, they satisfy IA.L2-3.5.3. The primary limitation is that OTP codes are not bound to the relying party, which means they remain vulnerable to real-time phishing attacks where an attacker captures and replays the code during its validity window. This does not make them non-compliant, but it does place them below FIDO2 and PIV in terms of assurance.

Authenticator Applications on Organization-Managed Devices

Time-based one-time password (TOTP) applications, including Microsoft Authenticator, Google Authenticator, and Duo Mobile, generate rotating codes on a mobile device. These applications function as something you have, provided the device running the application is under organizational control. In most

deployments, a centralized identity provider such as Microsoft Entra ID, Okta, or Duo Security manages MFA enrollment, enforcement, and logging across the organization.

The critical distinction is organizational management. An authenticator application running on an organization-issued or organization-enrolled device, where the organization can enforce screen lock policies, require encryption, and remotely wipe the device if necessary, is a defensible MFA implementation. The same application running on an unmanaged personal device raises significant compliance concerns, which the following section addresses in detail.

Push Notification Authentication

Push-based authentication, where the identity provider sends an approval request to a registered device, is a variant of the authenticator application model. The user receives a notification and approves the login attempt with a tap. Some implementations add number matching, where the user must enter a code displayed on the login screen into the authenticator application, to mitigate push fatigue attacks.

Push authentication is acceptable for CMMC environments when deployed on organization-managed devices and when the implementation includes number matching or equivalent anti-phishing measures. Organizations should ensure that their identity provider configuration logs all push authentication events for audit purposes.

The Personal Device Problem

Many small and mid-size contractors default to using employees' personal cell phones as the second authentication factor. An employee installs an authenticator application on a personal phone, and the organization considers MFA implemented. This approach is high-risk and difficult to defend under assessment scrutiny.

While NIST SP 800-171 does not contain a single statement that explicitly prohibits personal phones as authenticators, several controls working together make it very difficult to justify their use within the assessment boundary.

AC.L2-3.1.18 requires organizations to control the connection of mobile devices to organizational systems. If a personal phone is functioning as part of the authentication chain for CUI-scoped systems, the organization must demonstrate control over that device. On a personal phone without Mobile Device Management enrollment, that control is limited or nonexistent.

AC.L2-3.1.19 requires encryption of CUI on mobile devices. While an authenticator application does not store CUI in the traditional sense, the authentication secrets (TOTP seeds, push notification tokens) represent sensitive configuration data tied to CUI-scoped systems. These secrets are not explicitly classified as CUI, but under assessment scrutiny, an assessor may reasonably question whether adequate protections exist for that data on an unmanaged device.

The Media Protection (MP) family adds further requirements around organizational control of devices that interact with the protected environment. When considered together, the weight of these controls creates a defensible expectation that the organization should have authority over any device that plays a role in accessing CUI-scoped systems. This is an interpretation drawn from the interplay of multiple controls rather than an explicit regulatory prohibition, but it is the interpretation that assessors are most likely to apply.

A counterargument exists. If the phone is only generating a six-digit TOTP code and never touches CUI directly, one could argue it falls outside the CUI boundary, functioning no differently than a disconnected hardware token. That argument has

surface-level logic, but it weakens under assessment scrutiny. The assessor will ask whether the organization can revoke the authenticator if the employee leaves. The assessor will ask whether the device enforces a screen lock. The assessor will ask what happens if the phone is lost or stolen. On an unmanaged personal device, the answers to those questions are unsatisfying.

The defensible position is to use organization-issued or organization-managed devices for any authentication function within the CMMC boundary. For organizations where issuing phones is not practical, hardware security keys or hardware OTP tokens eliminate the personal device question entirely.

USB Port Policy and Hardware Authenticators

Organizations that select USB-connected hardware tokens or FIDO2 keys as their MFA solution will encounter an immediate tension with their media protection controls. MP.L2-3.8.7 requires organizations to control the use of removable media on system components, and many contractors implement this requirement by disabling USB ports entirely, either through BIOS settings, Group Policy, or physical means.

That approach creates a direct conflict. If all USB ports are disabled, the organization cannot use USB-connected authentication devices, which are among the strongest MFA options available.

The resolution lies in understanding that MP.L2-3.8.7 requires control of removable media, not the blanket elimination of all USB functionality. USB devices are classified by device class at the protocol level, and modern endpoint management tools can differentiate between device classes with precision. A properly configured endpoint can permit Human Interface Device (HID) class and Smart Card class connections while blocking USB Mass Storage class devices.

USB Device Classes Relevant to MFA

The three USB device classes relevant to this discussion each require a different policy treatment.

HID (Human Interface Device), Class 03. This is the device class used by FIDO2 security keys, including the YubiKey series. FIDO2 keys present themselves to the operating system as HID devices, not as storage. The policy recommendation is to allow this class for approved device models.

Smart Card, Class 0B. This class covers PIV and CAC card readers as well as some RSA token models that interface through the smart card protocol. Like HID, this class does not involve data storage. The policy recommendation is to allow this class for approved device models.

Mass Storage, Class 08. This is the device class used by USB flash drives, external hard drives, and other removable storage media. It is the class that MP.L2-3.8.7 is primarily concerned with. The policy recommendation is to block this class entirely.

Configuring Granular USB Control

On Windows endpoints, Device Installation Restrictions in Group Policy provide the mechanism for class-level USB control. The relevant policy path is Computer Configuration, Administrative Templates, System, Device Installation, Device Installation Restrictions. Within this path, the organization can configure policies to allow installation of devices that match specific device setup class GUIDs while preventing installation of all devices not described by other policy settings.

The key Group Policy Object settings are as follows. "Allow installation of devices that match any of these device setup classes" should include the GUIDs for HID ({745a17a0-74d3-11d0-b6fe-00a0c90f57da}) and Smart Card ({50dd5230-ba8a-11d1-bf5d-0000f805f530}) device classes. "Prevent installation of devices not described by other policy settings" should be enabled to create a default-deny posture for all other USB device types.

For organizations requiring tighter control, an additional layer of restriction is available through device instance ID policies. Rather than allowing all HID devices, the organization can restrict USB connections to specific hardware models by vendor ID and product ID. This means the policy permits a specific model of YubiKey while blocking other HID devices that the organization has not approved.

Endpoint management platforms including Microsoft Intune, Microsoft Endpoint Configuration Manager, and CrowdStrike Falcon Device Control offer equivalent or more granular controls with centralized reporting. These platforms also simplify the evidence collection process during assessment, because the configuration policies and compliance reports are readily exportable.

What the Assessor Will Expect

An assessor evaluating both IA.L2-3.5.3 and MP.L2-3.8.7 will look for three things. First, a written policy that defines which USB device classes are permitted and which are blocked, with a rationale that addresses how MFA hardware is accommodated. Second, a technical implementation, whether Group Policy export, Intune policy configuration, or equivalent, that matches the written policy. Third, evidence that the controls are functioning as intended, which may include test results showing that an unauthorized USB storage device is blocked while the approved authentication device is accepted.

Organizations that have disabled USB ports through physical means, such as epoxy or port covers, or through BIOS-level blanket disabling, will need to reconsider that approach if they intend to use USB-connected authenticators. The assessment requires demonstrating both effective MFA and effective media protection. Planning these two controls together, rather than in isolation, avoids the situation where satisfying one requirement undermines another.

The Restricted Authenticator Question

NIST SP 800-63B classifies SMS-based and voice-based one-time passwords as "restricted authenticators." This classification acknowledges that while these methods do provide a second factor, they carry known vulnerabilities that stronger authenticator types do not share.

SMS messages traverse the public switched telephone network and are susceptible to interception through SS7 protocol vulnerabilities, SIM swapping attacks, and social engineering of mobile carrier support staff. Voice-based OTP delivery shares similar exposure. These are not theoretical risks. SIM swapping attacks have been documented extensively in federal law enforcement actions and industry incident reports.

Under CMMC, an SMS-based second factor is not explicitly prohibited. An assessor is unlikely to issue a finding solely because the organization uses SMS-based MFA, provided that the implementation otherwise satisfies IA.L2-3.5.3. However, organizations should understand that the federal direction of travel is away from SMS as an authentication factor. OMB Memorandum M-22-09, which establishes the federal Zero Trust strategy, mandates phishing-resistant MFA for federal agencies. While M-22-09 does not directly apply to CMMC, it signals the standard that the Department of Defense considers appropriate for protecting sensitive information.

The practical recommendation is to avoid SMS-based MFA for CMMC-scoped systems if alternatives are available. FIDO2 keys, authenticator applications on managed devices, and hardware OTP tokens all provide stronger assurance at comparable or lower cost. Organizations currently using SMS-based MFA should plan a migration path toward phishing-resistant methods.

Related Controls That Shape MFA Implementation

MFA does not exist in isolation within the CMMC control set. Several additional controls directly affect how MFA must be deployed, monitored, and maintained.

IA.L2-3.5.2 requires authentication of users, processes, and devices as a prerequisite to allowing access. This control establishes the broader authentication framework within which MFA operates. The organization must be able to identify and authenticate every entity accessing CUI-scoped systems, not just human users.

SC.L2-3.13.8 requires encryption of CUI in transit. The session carrying the authentication exchange must be encrypted. If MFA credentials traverse an unencrypted channel, the authentication assurance is fundamentally undermined regardless of how strong the individual factors are.

AU.L2-3.3.1 requires the creation of system audit logs sufficient to support monitoring, analysis, investigation, and reporting. Authentication events, including successful logins, failed attempts, and MFA challenge results, must be captured in audit logs. The organization should verify that its identity provider and MFA solution generate logs that include the authentication method used, the timestamp, the user identity, and the outcome.

AC.L2-3.1.1 requires limiting system access to authorized users and to the types of transactions and functions those users are authorized to execute. MFA is one mechanism by which the organization enforces this access limitation, and the MFA deployment should align with the access control policy to ensure that privilege levels correspond to authentication strength.

MFA Selection: A Planning Framework

The following summaries evaluate each major authenticator option against the criteria that matter most for CMMC compliance and practical deployment: phishing resistance, managed device dependency, USB port requirements, relative cost, and the strength of the evidence the method produces during assessment.

FIDO2 Security Keys. Phishing-resistant. Does not require a managed mobile device. Connects via USB, NFC, or Bluetooth, so USB port dependency varies by model. Low cost, typically forty to sixty dollars per key. Produces strong assessment evidence because the identity provider logs clearly reflect hardware key authentication. For most small and mid-size contractors, FIDO2 keys offer the best combination of assurance, simplicity, and cost.

PIV/CAC Smart Cards. Phishing-resistant. Does not require a managed mobile device, but does require a card reader, which introduces a USB port dependency. Medium cost when factoring in card issuance, certificate management, and reader hardware. Produces strong assessment evidence. Most applicable to contractors already operating within federal programs that issue PIV or CAC credentials.

Hardware OTP Tokens. Not phishing-resistant, because OTP codes are not bound to the relying party and can be captured in real-time phishing attacks. Does not require a managed mobile device. USB port dependency varies by model. Medium cost. Produces strong assessment evidence because the token is a discrete, auditable device. A proven option, though less resistant to modern attack techniques than FIDO2 or PIV.

TOTP Authenticator Applications on Managed Devices. Not phishing-resistant. Requires an organization-managed mobile device, which means the organization must invest in Mobile Device Management infrastructure or issue dedicated phones. No USB port dependency. Low cost for the software itself, though the managed device requirement adds overhead. Produces moderate assessment evidence, because the assessor must verify both the authenticator configuration and the device management posture.

Push Notification Authentication on Managed Devices. Partially phishing-resistant when the implementation includes number matching or equivalent challenge-response measures. Requires an organization-managed mobile device. No USB port dependency. Low to medium cost. Produces moderate assessment evidence. Organizations deploying push authentication should ensure that number matching is enabled and that push fatigue protections are in place.

SMS OTP (Restricted Authenticator). Not phishing-resistant. Does not require a managed device or USB port. Low cost. Produces weak assessment evidence because of the known vulnerabilities documented in NIST SP 800-63B, including SIM swapping and SS7 interception. While not explicitly prohibited under CMMC, SMS-based MFA is the least defensible option and should be avoided if alternatives are available.

Organizations should select their MFA approach based on the intersection of security assurance, operational feasibility, and the ability to produce clear assessment evidence. For organizations that prefer application-based authentication, the investment in a managed device infrastructure is a prerequisite that should be weighed against the simplicity of hardware keys.

Sample System Security Plan Entry for IA.L2-3.5.3

The following is a representative SSP entry for IA.L2-3.5.3 that an organization could adapt to its own environment. A well-written SSP entry for this control should identify the specific authenticator types in use, describe how they satisfy the two-factor requirement, reference the supporting policies and configurations, and address both privileged and non-privileged access scenarios.

SSP Field	Content
Control Identifier	IA.L2-3.5.3
Control Text	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
Implementation Status	Implemented
Implementation Description	All accounts within the CMMC assessment boundary authenticate using a password and a FIDO2 hardware security key. [Identity Provider Name, e.g., Microsoft Entra ID, Okta, Duo Security] serves as the centralized identity provider, configured to require FIDO2 key registration. Single-factor authentication is disabled for all in-scope accounts. Privileged accounts require MFA for both local and network access. Non-privileged accounts require MFA for all network access. Each user is issued two FIDO2 keys: a primary key and a backup stored in a secured location. Key issuance and revocation are tracked in the asset inventory. Group Policy permits HID (Class 03) and Smart Card (Class 0B) USB device classes while blocking Mass Storage (Class 08), aligning MFA hardware with removable media controls under MP.L2-3.8.7. Authentication events, including MFA outcomes, are logged and forwarded to the centralized log repository in support of AU.L2-3.3.1.

Related Policies	Access Control Policy, Identification and Authentication Policy, Media Protection Policy
Supporting Evidence	Identity provider MFA configuration screenshots; GPO export showing USB device class restrictions; sample authentication log entries showing MFA completion; FIDO2 key issuance and inventory records; test results confirming single-factor login attempts are rejected

This sample reflects a FIDO2-based implementation. Organizations using other authenticator types should adjust the implementation description to reflect their specific MFA solution, identity provider, and supporting infrastructure. The key elements that any SSP entry for this control must address are the specific factor types in use, the scope of coverage across privileged and non-privileged accounts, the enforcement mechanism that prevents single-factor access, and the connection to related controls.

One area that organizations frequently overlook during assessment preparation is the key issuance and revocation record referenced in the sample above. Assessors will want to see documented evidence that each hardware authenticator has been provisioned, assigned to a specific user, and tracked as an organizational asset. Equally important is the revocation process: when an employee departs or changes roles, the organization must demonstrate that their authenticator was deregistered from the identity provider and either recovered or deactivated. Without this documentation, the organization may have a functioning MFA deployment but lack the evidence to prove it is managed.

MFA and the Plan of Action and Milestones

Organizations should understand that IA.L2-3.5.3 is, in practice, not a control that lends itself to deferral through a Plan of Action and Milestones (POA&M). While the CMMC Final Rule and associated assessment guidance establish a limited conditional certification pathway, the practical treatment of MFA by assessors makes deferral an extremely high-risk approach.

The CMMC Final Rule does allow a conditional certification pathway in which an organization may carry a small number of NOT MET findings on a POA&M, provided the organization meets a minimum assessment score threshold and closes all POA&M items within 180 days. However, not all controls are eligible for this pathway. The Department of Defense has established scoring criteria and restrictions that effectively exclude certain high-impact controls from POA&M deferral. While the DoD has not published a single definitive list titled "automatic fail controls," the scoring model treats MFA as a high-value control, and the consistent position across assessors and the practitioner community is that a NOT MET finding on IA.L2-3.5.3 is not compatible with certification.

The logic is straightforward. Without MFA, every account accessing CUI-scoped systems is protected by a single factor, typically a password. Passwords are subject to credential stuffing, brute force attacks, phishing, and reuse across services. An organization operating without MFA has a fundamental gap in its access control posture that cannot be offset by strength in other control areas.

What this means in practical terms is that MFA should be fully implemented and operational before the organization enters the assessment process. An organization that begins a CMMC Level 2 assessment with password-only authentication on any in-scope system is highly likely to receive a NOT MET finding for IA.L2-3.5.3, and under current assessment practice, that finding alone is generally sufficient to prevent certification.

Organizations in the early stages of CMMC readiness should prioritize MFA deployment accordingly. It is one of the first controls that should be implemented, tested, and documented, not one of the last.

Conclusion

Multifactor authentication is not optional under CMMC Level 2. Under current assessment practice, it is not a control that can be deferred to a Plan of Action and Milestones with the expectation that assessors will accept a future commitment. Organizations entering the assessment process with password-only authentication are unlikely to achieve certification.

The technical implementation of MFA requires coordination across multiple control families. The authenticator type selected must be compatible with the organization's media protection policy, mobile device management posture, audit logging configuration, and access control architecture. Planning these elements together, early in the compliance readiness process, prevents the conflicts that arise when controls are implemented independently.

The strongest and most assessment-ready MFA options available today are FIDO2 security keys and PIV smart cards. Both are phishing-resistant, produce clear audit evidence, and do not depend on managed mobile devices. For organizations seeking the most straightforward path to a defensible MFA implementation, these options should be the starting point.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of David Koran & Associates, a CMMC consulting practice serving Defense Industrial Base contractors and their legal counsel. The firm provides readiness, enablement, and implementation services for organizations pursuing CMMC certification. He is an Associate Member of the ABA Section of Public Contract Law. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

National Institute of Standards and Technology. (2020). NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

National Institute of Standards and Technology. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management. https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology. (2015). NIST Special Publication 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials. https://csrc.nist.gov/publications/detail/sp/800-157/final

Office of Management and Budget. (2022). Memorandum M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

FIDO Alliance. (2024). FIDO2: Web Authentication (WebAuthn) Specifications. https://fidoalliance.org/fido2/

USB Implementers Forum. (2024). USB Device Class Specifications. https://www.usb.org/defined-class-codes

Microsoft. (2024). Manage Device Installation with Group Policy. https://learn.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy

Cyber AB. (2025). CMMC Assessment Guide Level 2, Version 2.13. https://cyberab.org/

Department of Defense. (2024). Cybersecurity Maturity Model Certification (CMMC) Program Final Rule, 32 CFR Part 170. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program