ZIMPERIUM®

Cybersecurity Maturity Model Certification:

The Mobile Device Requirements, and How to Address Them

Executive Summary

To comply with Cybersecurity Maturity Model Certification requirements, organizations need to ensure a comprehensive set of security controls are in place, and this includes protections against the risks posed by the use of mobile devices. This ebook offers a detailed look at how CMMC requirements pertain to mobile technologies, and it reveals how mobile threat defense solutions now represent a critical tool for addressing these requirements.

An Introduction to Cybersecurity Maturity Model Certification

To meet its charter in safeguarding the nation, the U.S. Department of Defense (DoD) needs to safeguard its data. Therefore, it's an imperative for agency staff and its contractors to establish and sustain robust cybersecurity measures.

In order to normalize and standardize cybersecurity preparedness among its contractors, the DoD launched the Cybersecurity Maturity Model Certification (CMMC) program. Through this program, the DoD is seeking to establish a standardized way to measure their defense contractors' capabilities, readiness, and sophistication in the area of cybersecurity. Now in its second iteration, the CMMC has three different tiers:

- **Level 1:** The foundational level, is focused on companies that only manage federal contract information (FCI).
- **Level 2:** The advanced level, applies to companies with controlled unclassified information (CUI).
- **Level 3:** The expert level, applies to the highest-priority programs that store or manage CUI.

The DoD is now starting to require certification with certain contracts. Ultimately, CMMC requirements may start to apply to all government contractors. Consequently, for defense industrial base (DIB) contractors that serve the DoD, it is now vital to establish the cybersecurity capabilities that align with the CMMC. This includes addressing the specific risks and requirements associated with mobile devices.

As teams look to establish mobile device security, it is important to go beyond taking a bare-minimum approach to compliance, and instead take a proactive, holistic approach that sets the stage not only for near-term compliance but long-term security. In the following sections, we'll look at some of the underlying requirements of CMMC and how they apply to mobile technologies. We'll then look at some core technologies and approaches that teams will need to employ in order to address these requirements.

CMMC 2.0	Model	Assessment
LEVEL 3 Expert	**110+** **Practices based on NIST SP 800-172**	• **Meet Level 2 compliance** • **Implement still-in-review subset of controls from NIST SP 800-172** • **Engage in triennial government-led assessment**
LEVEL 2 Advanced	**110** **Practices aligned with NIST SP 800-171**	• **Implement the 110 controls in NIST SP 800-171** • **Engage in triennial assessment conducted by a third-party Certified Third-Party Assessment Organization (C3PAO)** • **Submit an annual self-assessment**
LEVEL 1 Foundational	**17** **Practices**	• **Implement 17 CMMC practices that map to NIST SP 800-171 and outlinedFAR 52.204-21** • **Submit an annual self-assessment to the DoD**

CMMC and NIST Standards, and How They Apply to Mobile Technologies

CMMC requirements are aligned with National Institute of Standards and Technology (NIST) Special Publications (SP). Level two is aligned with NIST SP 800-171, and level three uses a subset of NIST SP 800-172 requirements. These documents catalog a comprehensive set of security controls that must be applied to protect CUI.

For level two and three, at least 110 practices based on NIST standards must be addressed. In addition, these documents also reference other standards documented by NIST. In order to effectively address CMMC standards, it is vital to understand these various documents and the relevant context and guidance they provide.

Access Control

CMMC Practice AC.L2-3.1.18: Controlling Mobile Device Connections

The CMMC Level 2 Assessor Guide guides CMMC audits and includes this practice: "AC.L2-3.1.18 – Mobile Device Connection." This section requires you to control the connections of mobile devices. As part of the assessment objectives, CMMC Certified Assessors (CCAs) needs to determine if:

- Mobile devices that process, store, or transmit CUI are identified
- Mobile device connections are authorized
- Mobile device connections are monitored and logged

Since these objectives are vague, the assessor guide includes two additional references. First, it points you to NIST SP 800-171, section 3.1.18. Additionally, it includes a discussion of NIST SP 800-171, which notes, "Many controls for mobile devices are reflected in other CUI security requirements. NIST SP 800-124 provides guidance on mobile device security." [1]

NIST SP 800-171: Control Connection of Mobile Devices

NIST 800-171 includes a section on access control requirements, including 3.1.18. In the discussion, NIST outlines the following usage restrictions and implementation guidance for mobile devices:

- Device identification and authentication
- Configuration management
- Implementation of mandatory protective software (e.g., malicious code detection, firewall)
- Scanning devices for malicious code
- Updating virus protection software
- Scanning for critical software updates and patches
- Conducting primary operating system (and possibly other resident software) integrity checks
- Disabling unnecessary hardware (e.g., wireless, infrared)

CMMC Multi-Factor Authentication

The CMMC Assessment Guide for Level 2 states, "Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts." [2]

From here, the assessment guide points you to NIST SP 800-171, section 3.5.3.

NIST SP 800-171: Identification and Authentication (IA) Control Family

Within the IA control family, NIST outlines the steps required to ensure that users accessing networks are who they say they are.
The NIST requirement defines multi-factor authentication (MFA) as a combination of two or more of the following:

- Something you know (a password)
- Something you have (a token or mobile device)
- Something you are (a biometric like fingerprint or face ID)

Teams should also note that NIST 800-171 explains the following:
"In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security."

Configuration Management

CMMC Configuration Management Practices: How They Apply to Mobile

The CMMC Assessment Guide for Level 2 details the technical system security requirements for hardware, software, and firmware. To be compliant, organizations need to implement controls that align with the following practices:

- CM.L2-3.4.1 – System Baselining: Establish and implement secure baseline configurations.
- CM.L2-3.4.2 – Security Configuration Enforcement: Establish and enforce security configuration settings.
- CM.L2-3.4.3 – System Change Management: Track, review, approve or disapprove, and log changes to systems.
- CM.L2-3.4.4 – Security Impact Analysis: Analyze security impact prior to implementing changes.
- CM.L2-3.4.5 – Access Restrictions for Change: Define, document, approve, and enforce physical and logical access restrictions associated with changes.
- CM.L2-3.4.6 – Least Functionality: Configure systems so they provide only essential capabilities.
- CM.L2-3.4.7 – Nonessential Functionality: Restrict, disable, or prevent the use of non-essential programs, functions, ports, protocols, and services.
- CM.L2-3.4.8 – Application Execution Policy: Apply deny-by-exception policy to prevent unauthorized software usage with permit-by-exception for authorized software usage.
- CM.L2-3.4.9 – User Installed Software: Control and monitor user-installed software.

Typically, teams know that they need to manage configurations for traditional devices, such as workstations and routers. However, the CMMC Assessment Guide specifically calls out mobile devices in the discussion section for these practices:

- CM.L2-3.4.1 – System Baselining
- CM.L2-3.4.3 – System Change Management

Since the guide includes mobile devices as part of system baselining and change management, teams should infer that all these practices must be applied to mobile endpoints.

NIST 800-171: Configuration Management Controls

Level 2 CMMC standards map to NIST 800-171 requirements. When looking at the configuration management control family, the first basic security requirement is 3.4.1:
“Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.”

In the discussion, this publication refers to SP 800-128 for guidance on security-focused configuration management.

Applying Standards to Mobile

NIST SP 800-128: Updates Reflect Increased Focus on Mobile

When NIST updated SP 800-128 in 2019, the agency included four new references to mobile devices, which it listed as substantive.[3] This included retitling NIST SP 800-124, “Guidelines for Managing the Security of Mobile Devices in the Enterprise.”[4] The authors also replaced “personal computers” with “endpoints (e.g., laptops, desktops, mobile devices).”
Fundamentally, this shift in language and focus shows that NIST recognized mobile devices as critical to productivity and security.

NIST SP 800-124 and NIST SP 1800-4B: Underscoring the Unique Risks of Mobile Devices

NIST SP 800-124 and NIST SP 1800-4B discuss the unique security risks that mobile devices pose to an organization’s networks and systems. Although the two use slightly different language, both reference mobile threats that teams need to consider when implementing their CMMC configuration management controls.

NIST SP 1800-4B, section 3.4, “Risk Assessment,” outlines the following common threats to mobile devices:[5]

- Mobile malware
- Social engineering
- Stolen data due to loss, theft, or disposal
- Unauthorized access
- Electronic eavesdropping
- Electronic tracking
- Access to data by legitimate third-party applications

Further, in 3.4.2, NIST SP 1800-4B details the vulnerabilities commonly associated with mobile applications, including those installed by device owners, carriers, and as part of operating system bundles.

Why Mobile Threat Defense Capabilities Are a Requirement for CMMC

Understanding the Different Mobile Security and Management Technologies

NIST recognizes that mobile devices and their security requirements have changed significantly over the last ten years. In NIST SP 800-124, "Overview of Mobile Security Technologies," the agency defines different enterprise mobile security technologies.

In its definitions, NIST outlines three mobile security technologies that people often view as interchangeable, explaining how they deliver unique capabilities:

- **Mobile device management** (MDM) enables deployment, configuration, and active management for mobile devices.
- **Mobile application management** (MAM) enables the establishment and enforcement of fine-grained control over different apps on a single managed device.
- **Mobile threat defense** (MTD) enables detection of malicious apps, network-based attacks, improper configurations, and known vulnerabilities in mobile apps or the mobile OS.

MTD Addresses the Limitations of MDM

MDM enables you to provision devices and set basic configurations on devices that you manage. However, it lacks capabilities that can monitor and detect:

- Mobile phishing attacks that install malicious code on devices
- Malicious applications downloaded from untrusted sources
- Real-time device health
- Cloud application security
- Advanced threats

MTD fills in the gaps that MDM and MAM leave behind, providing the robust mobile device security that teams need to achieve CMMC compliance.

NIST 800-124 distinguishes MTD from MDM and MAM in section 4.2.3 "Mobile Threat Defense," by outlining the following MTD capabilities:

- Real-time continuous monitoring
- Assessing apps after deployment and during runtime
- Detecting and protecting mobile devices, apps, and end users against attack via wireless network
- Detecting attacks against an app or OS software, such as side-loaded apps
- Detecting and alerting users to unexpected interactions among apps or the use of data on the device

With these capabilities, MTD supplements your MDM and MAM tools, enabling you to take a comprehensive approach to mobile security.

MTD Addresses the Limitations of Patch Management

MDM enables you to provision devices and set basic configurations on devices that you manage. However, it lacks capabilities that can monitor and detect:

- Mobile phishing attacks that install malicious code on devices
- Malicious applications downloaded from untrusted sources
- Real-time device health
- Cloud application security
- Advanced threats

MTD fills in the gaps that MDM and MAM leave behind, providing the robust mobile device security that teams need to achieve CMMC compliance.

NIST 800-124 distinguishes MTD from MDM and MAM in section 4.2.3 “Mobile Threat Defense,” by outlining the following MTD capabilities:

- Real-time continuous monitoring
- Assessing apps after deployment and during runtime
- Detecting and protecting mobile devices, apps, and end users against attack via wireless network
- Detecting attacks against an app or OS software, such as side-loaded apps
- Detecting and alerting users to unexpected interactions among apps or the use of data on the device
- With these capabilities, MTD supplements your MDM and MAM tools, enabling you to take a comprehensive approach to mobile security.

MTD Addresses the Limitations of Patch Management

Mobile device vulnerabilities and threats become more challenging as teams look at them through the lens of CMMC configuration management practices. Installing operating system and app security updates enables teams to meet some configuration management requirements. However, the reality is that patching falls far short of meeting CMMC standards and establishing robust security.

There are a couple key reasons for this. First, patching isn’t always an option. Security personnel may have no control over personal mobile devices, including whether their OSs are on the latest version, which apps are downloaded, and whether apps are updated in a timely manner or at all. Even when looking at company-owned devices, apps that come pre-installed from carriers and apps bundled with operating systems can jeopardize compliance.

Second, significant time can elapse between when vulnerabilities are identified and when a patch is even available, let alone installed. The reality is that vendors in the mobile device ecosystem, including both device manufacturers and app providers, may not deliver patches in a timely manner once vulnerabilities have been identified. For example, news reports indicated that it took Apple more than six months to address several zero-day vulnerabilities that had been discovered.[6] A researcher detected these vulnerabilities in iOS versions 14 and 15, which meant millions of users were exposed.

This is compounded by the well-documented delays in getting patches installed. One report found that businesses take an average of 215 days to patch a reported vulnerability, and even for critical vulnerabilities, it often takes six months for patching to be completed.[7] When you consider that more than one-third of the zero-days discovered specifically targeted mobile devices, this represents a significant exposure, both from a security and CMMC compliance standpoint.[8]

MTD delivers comprehensive configuration management controls that help organizations maintain secure configurations for mobile apps and operating systems. By delivering real-time, on-device protections, MTD enables teams to protect mobile devices and applications, even if they lack the latest patches and updates. Advanced MTD solutions deliver real-time mobile device analysis and logging, providing visibility into:

- Device weaknesses
- OS vulnerabilities
- Network attacks
- Phishing attacks
- Application vulnerabilities

This continuous device attestation capability ensures that organizations can implement and, more importantly, enforce secure configuration baselines across their mobile device fleet, including user-owned devices.

MTD Addresses the Limitations of MFA

MFA will always be an important security control. It acts as a secondary line of protection at the identity layer. However, malicious actors have recently found ways to bypass this control through sophisticated SMS-based attacks. Following are a couple examples:

- **Supply chain attacks.** In August 2022, threat actors deployed attacks against Cloudflare and Twilio.[9] As part of these sophisticated SMS-based spear phishing attacks, malicious actors texted employees a password reset notification along with a well-disguised link. Additionally, the end-to-end encryption messaging service, Signal, was one of the 125 customers impacted by the attack, ultimately causing a downstream impact to roughly 1900 of its customers. CMMC exists precisely because the interconnected nature of the DIB means that one impacted contractor creates a flow-down supply chain data security risk.
- **MFA-bombing attacks.** As organizations implement MFA, attackers seek ways around it. In an MFA bombing attack, also called MFA push spam or MFA fatigue, attackers overwhelm users by sending high volumes of text messages, waiting for the user to accept the authentication attempt to stop the notifications. In September 2022, attackers used this tactic against Uber, infecting a third-party contractor's personal device with malware that exposed and compromised credentials.[10]

With the rise of these sophisticated attacks, DIB members need additional controls that reinforce their MFA protections. It is imperative that you take into account how threat actors can circumvent your controls as part of CMMC compliance. It is crucial to implement MFA, but you should also reinforce your security controls to mitigate these new risks.

MTD offers the critical safeguards that supplement MFA. As mentioned above, MTD delivers such capabilities as real-time, continuous monitoring and capabilities for detecting wireless network-, app-, and OS-based attacks.

NIST SP 800-124 lists MTD as a mitigation and countermeasure for several threats, including the exploitation of underlying vulnerabilities in devices, credential theft via phishing, and the installation of unauthorized certificates.

Key Advantages of Mobile Threat Defense Tools

MTD Can Supplement Security Awareness Training

Sophisticated MFA-based SMS spear phishing attacks incorporate threat intelligence on intended targets and send these individuals to specially crafted, legitimate-looking, malicious landing pages.

MTD supplements your security awareness training with behavioral and machine learning that detects device, network, phishing, and application mobile attacks, even when a device is not connected to the network.

MTD Mitigates Bring Your Own Device (BYOD) Risks

When employees use personal devices as part of your remote work model, they become the administrators, deciding when to upgrade their OS, which network connections to use, which apps to download, and so on.

Most people don't want to install an application that allows their employers access to their devices. MTD enables you to secure personal devices without compromising employee privacy. An MTD solution that detects threats on-device rather than sending information to a cloud secures mobile devices without the need to collect or process personally identifiable information (PII).

MTD enables you to secure employee-owned devices so that you can implement and maintain CMMC compliance across all devices that connect to your networks.

MTD Mitigates Mobile Operating System (OS) Risks

A mobile device's OS often comes with vulnerabilities and can be open to misconfigurations. MDM and MAM lock down your devices and deploy security policies. MTD augments and completes your mobile device security program by overcoming threats arising from malicious links embedded in SMS-based phishing attacks. Distracted users with small smartphone screens may not be able to determine whether the link is malicious because they can't just use the "hover" capability that they would with a mouse. MTD closes this security gap, enabling robust security and CMMC compliance.

MTD Protects Mobile Devices' Expanded Attack Surface

Both the nature of cyberattacks and the CMMC standards make clear that mobile endpoints need to be secured—just as traditional laptops and desktops. However, to date, many organizations have failed to secure the mobile component of their attack surface.

Each mobile device is a potential attack vector that is part of a larger attack chain. In an SMS-based spear phishing attack, reconnaissance includes gathering information about employees and services, then communicating with these individuals. Leveraging malicious websites, they then compromise credentials, which can lead to enterprise system access. MTD closes the security gap that MDM and MAM create by providing visibility into the threats targeting mobile endpoints. With MTD, you can reduce your mobile device attack surface.

How Mobile Threat Defense from Zimperium Can Support CMMC

ITo comply with CMMC Assessment Objectives, you need to give your CCA the documentation proving that you have a comprehensive approach to mobile device security. Finding the right set of technologies that protect CUI and ensure continued CMMC compliance poses a challenge for most organizations. However, with Zimperium MTD solutions, you can streamline your mobile device security—so you can achieve your top-level security, compliance, and organizational objectives.

Access Control	Wireless protection and response. On device zero-day protection software.
Awareness and training	Realtime device alerts to users for risk awareness. User education for risks of sms/email phishing and side loaded App risks.
Configuration Management	Mobile Application Vetting (MAV).
Identification Authentication	Mapping the mobile device threat to the user. Providing the threat signal from the device to the EMM ensures device health and compliance.
Incident response	Record incident status and forensic detail specific to mobile devices. On-device threat response. Mapping mobile threat trends and response actions.
Risk Assessment	Mobile app vetting and on device App monitoring. Risk assessment of custom App development in the development life cycle.
System & Information Integrity	Provides ongoing protection against malicious code.

Zimperium MTD

Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - is an advanced MTD solution for enterprises, government agencies, and contractors in the DIB sector. With this solution, your organization can establish the mobile device security controls that comply with CMMC standards and deliver advanced protections. To safeguard CUI against mobile threats and risks, MTD detects mobile threats, notifies security teams of incidents, and blocks unauthorized access to resources. Used by many government agencies, including the DoD, Zimperium was the first MTD provider to be granted an Authority to Operate (ATO) status from the Federal Risk and Authorization Management Program (FedRAMP).

With Zimperium MTD, your organization can leverage the only on-device mobile threat defense solution that protects CUI across Android, iOS, and ChromeOS devices. The solution offers robust safeguards against known and zero-day, advanced persistent threats. MTD keeps mobile devices secure—without relying on cloud-based lookups, content scanning, or other privacy-invasive techniques.

On-Device Detection Powered by z9

MTD is powered by Zimperium's z9, a dynamically updatable engine. z9 offers behavioral and machine learning techniques that detect device, network, phishing, and mobile application attacks, without having to rely on updates or an active network connection. Zimperium z9 can quickly detect both unknown and known malicious applications and activity, along with their malware family (Exploit, Hacktool, Spyware, Riskware, Banker, Adware, Trojan, Generic Malware).

Zimperium's Advanced App Analysis

Zimperium's Advanced App Analysis (z3A) enables MTD to perform in-depth mobile application scanning for privacy and security risks. z3A Mobile Application Vetting (MAV) is designed to rigorously analyze apps using an array of analytical engines and intelligence sources to identify data leakage, malware, C&C communications, vulnerabilities, etc. The app reporting provides deep intelligence, including contextual analysis, libraries and app communications with countries of origin. The solution delivers detailed privacy ratings, malware classifications, security ratings, and customizable app privacy settings.

Conclusion

For organizations that manage the CUI of the DoD—or any other government agency—the time to establish strong mobile device security is now. With MTD, your organization can institute the robust defenses you need to comply with CMMC requirements—and mitigate the advanced attacks targeting mobile device users and apps today. For more information on how Zimperium MTD or the Zimperium Mobile Application Protection Suite (MAPS) can help you meet CMMC requirements, contact us today.

Sources

1 NIST, SP 800-171 Rev. 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," February 2020 (includes updates as of January 28, 2021), URL: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

2 CMMC Assessment Guide, Level 2, Version 2.0, December 2021, URL: https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

3 NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems," URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

4 NIST, SP 800-124, Rev 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020, URL: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft

5 NIST SP 1800-4B, "Mobile Device Security: Cloud and Hybrid Builds," February 2019, URL: https://www.nccoe.nist.gov/publication/1800-4/VolB/index.html

6 Forbes, "Apple Ignored 3 Zero-Day iPhone Attacks For Months, Claims Researcher," Gordon Kelly, September 25, 2021, URL: https://www.forbes.com/sites/gordonkelly/2021/09/25/apple-iphone-warning-security-three-zero-day-attacks-new-iphone-hack/?sh=54744a057741

7 Orange, "Security Navigator 2023 shows Cyber Extortion dominates landscape as 40% is malware, attackers target Europe and beyond, and SMEs, manufacturing and the public sector particularly exposed," November 25, 2022, URL: https://newsroom.orange.com/security-navigator-2023-shows-cyber-extortion-dominates-landscape-as-40-is-malware-attackers-target-europe-and-beyond-and-smes-manufacturing-and-the-public-sector-particularly-exposed/

8 Zimperium, "2022 Global Mobile Threat Report: Key Insights on the State of Mobile Security," Richard Melick, March 14, 2022, URL: https://www.zimperium.com/blog/global-mobile-threat-report-key-insights/

9 The Hacker News, "Hackers Behind Twilio Breach Also Targeted Cloudflare Employees," Ravie Lakshmanan, Aug 10, 2022, URL: https://thehackernews.com/2022/08/hackers-behind-twilio-breach-also_10.html

10 Uber, "Security update," September 19, 2022, URL: https://www.uber.com/newsroom/security-update

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244