Enabling CMMC Compliance

Hypori
One Device, Zero Worries™

CMMC (Cybersecurity Maturity Model Certification) is a DoD (Department of Defense) program created to protect CUI (Controlled Unclassified Information) and FCI (Federal Contract Information) shared with U.S. defense contractors and subcontractors during contract performance.

The What and The Why

Cybersecurity is a priority for the DoD (U.S. Department of Defense), and it is top of mind for many of the contractors and subcontractors that comprise the DoD's multi-tier supply chain known as DIBs (i.e., the defense industrial base)[1].

These entities are actively being targeted with cyber-attacks from nation-states and other malicious actors whose goal is to steal intellectual property (e.g., FCI and CUI shared with DIBs. In response the DoD developed 32 CFR Part 170, or CMMC Program, which is now being used to assess existing DoD cybersecurity requirements, with the goal of strengthening DIB cybersecurity and better safeguarding DoD information.

One Device, Zero Worries

Hypori virtualizes **secure mobile access** from any endpoint device (e.g., a smartphone or tablet) to controlled apps and data residing in secure networks. The solution offers enterprise-grade security and total personal privacy, and unlike Mobile Application Management (MAM) solutions, Hypori never **transmits, stores, nor processes data** on an endpoint device.

Published on 15-OCT-2024, and **effective 16-DEC-2024**, CMMC language is included in contracts as of **1Q2025**. The 48 CFR part 204[2] CMMC Acquisition rule (updated 11-OCT-2024 – Section 204.7500) **allows the DoD to require adherence to a specific CMMC certification level in a solicitation or contract**.

When CMMC requirements are applied to a solicitation, contracting officers ***will not*** 1) make an award, 2) exercise an option, or 3) extend the period of performance on a contract, unless the offeror or contractor has passing results from a current certification assessment or self-assessment for the CMMC level.

An affirmation of continuous compliance with the security requirements in the **Supplier Performance Risk System** (SPRS) for all information systems that process, store, or transmit FCI or CUI during contract performance is also required. Furthermore, the appropriate CMMC certification requirements **will flow down to subcontractors** at all tiers when the subcontractor processes, stores, or transmits FCI or CUI.

[1] https://www.congress.gov/crs-product/IF10548
[2] https://www.ecfr.gov/current/title-48/chapter-2/subchapter-A/part-204

Hypori - Out of Scope (a good thing). Out of Mind.

Hypori's **CMMC Platform** protects customers from data loss due to a compromised edge device. It is deployed in AWS GovCloud using the Hypori **Government Platform** framework that was proven via many DoD, Commercial, Intelligence Community, and 3PAO security assessments of our component architecture. These reviews continue on a regular basis.

The **Hypori App** employs Virtual Mobile Infrastructure (VMI) technology that is technically equivalent to a Virtual Desktop Infrastructure (VDI). It is installed on an endpoint device and does not allow any processing, storage, or transmission of CUI or FCI. It can only transmit video streams as encrypted pixels and associated audio. Hypori embraces **Zero Trust** principles by not trusting the device and putting the architecture in place to guarantee trust. Hypori has excelled in many (10+) nation state level security assessments by the U.S. Military and Intelligence Communities, and FedRAMP 3PAO Red Teams[3].

Per Table 3 §170.19(c)(1) [**Level 2 – see below**], and Table 5 §170.19(d)(1) [**Level 3**] in 32 CFR Part 170, the way in which Hypori has implemented its Hypori VDI Client App results in **the endpoint device** on which it is hosted **being considered out-of-scope** by **CMMC**, and with no documentation requirements.

TABLE 3 TO § 170.19(c)(1)—CMMC LEVEL 2 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS

Asset category	Asset description	OSA requirements	CMMC assessment requirements
Assets that are not in the Level 2 CMMC Assessment Scope			
Out-of-Scope Assets	An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.	• Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI.	• None.

This means **an edge device running the Hypori App is not subject to a CMMC assessment**. As such, the Hypori App enables access to CUI and FCI from an endpoint device, including as part of a BYOD program, while eliminating any concerns that the endpoint device is designated as a contractor risk managed asset (CRMA) and thus subject to CMMC practices and assessments.

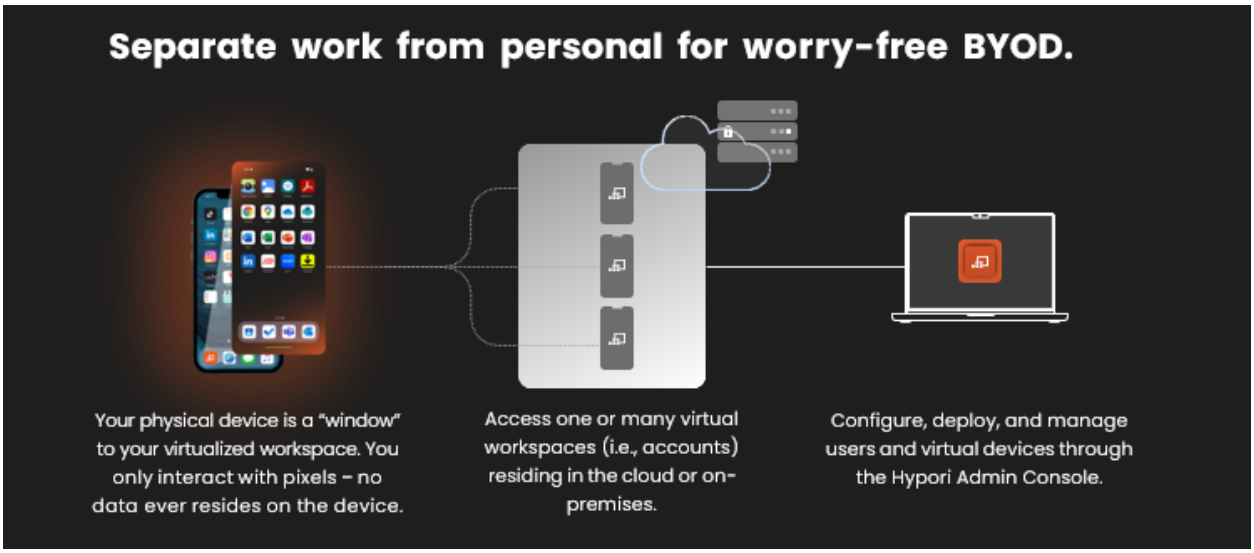
[3] Federal Risk and Authorization Management Program (FedRAMP) Third-Party Assessment Organization (3PAO); https://www.fedramp.gov/assessors/

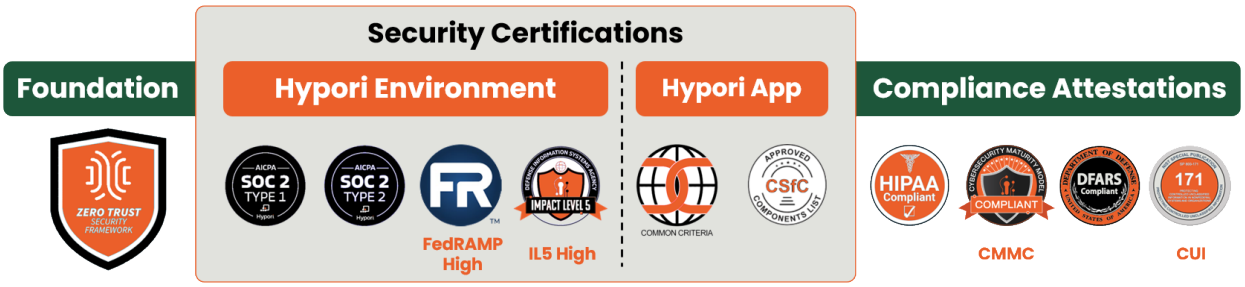
In contrast, edge devices that run **MAM solutions** and access CUI or FCI are considered **in-scope**. They classify as **Security Protection Assets** and require the implementation of all relevant **Level 2 practices**. The edge devices are likely to be considered a **contractor risk managed asset** (CRMA) which could trigger a CMMC assessment.

MAM also presents potential liability and exposure issues and may invade user privacy. For example, any edge device storing CUI will need to be sanitized (per NIST 800.88 - Guidelines for Media Sanitization) when that edge device leaves organizational control. For data categorized as 'moderate' that will require a 'purge' (see page 24 of NIST 800.88).

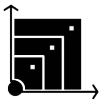
Some of these details were previously explored in the Hypori blog post entitled "SMB DIBS Guide to CMMC Compliance: Essential Checklist for Cybersecurity".

For more detailed technical information, including the **Hypori CMMC Cloud Shared Responsibility Model** that provides customers with the specific controls they inherit from the Hypori CMMC Cloud to comply with CMMC requirements, contact info@hypori.com. For current compliance information visit the Hypori Trust Center.





Please see the chart below for some additional features and benefits.

Features		Benefits	
	**Enterprise Grade Security built upon a Zero-Trust architecture.**		**Self-protection from mobile attack surfaces. Enables access to sensitive data.**
	**DoD doesn't have access to an end-user's personal workspace.**		**Provide 'Total (100%) Personal Privacy.' Worry-free BYOD!**
	**Secure Virtual Access (end-users only interact with encrypted pixels – not data).**		**Access apps and data remotely without exposing risks or potential liabilities.**
	**Zero-Trust Architecture. IL5, FedRAMP High, SOC 2, CSfC, Common Criteria.**		**Security certifications enable support for a range of secure remote access use cases.**
	**Data never transmitted to, stored, or processed on a mobile device.**		**Mitigate data loss and the need to wipe, confiscate, and/or subpoena a device.**
	**Multiple Mobile Devices (N:1) One Workspace.**		**Eliminates need to carry multiple mobile devices Licensing based upon # of virtual workspaces (i.e. accounts)– not number of mobile devices.**
	**One Device (1:N) Multiple workspaces.**		
	**Multiple Mobile Devices (N:N) Multiple Workspaces.**		
	**Execute apps/process data at "cloud resource speed".**		**Age/model of device and version of OS is irrelevant. Can extend a useful life.**
	**SaaS-based (AWS) with Hypori App downloaded from App stores.**		**Easily deploy and scale, with one customer supporting 50,000 users.**
	**Works on iOS and Android devices.**		**Device independent aside from mobile OS release levels.**
	**Decreases operational complexity. No additional hardware or software costs.**		**Minimize operational and financial impact on IT.**