CMMC Applies to Mobile Devices Too – Are You Prepared ?

The easiest way to adhere to the mobility requirements of CMMC is to simply not allow employees to use their personal devices to access CUI – correct ? Well not any longer!

If you are like most companies, your employees do not want to be forced to carry one device for work and a separate device for personal use. Additionally, the costs to acquire, distribute, maintain and recoup corporate owned devices could always be better spent elsewhere. …And then do you standardize on iOS or Android? Either way, a significant percentage of your user base is inconvenienced. Allowing BYOD while still adhering to CMMC requirements suddenly seems like an appealing approach.

But when it comes to CMMC and BYOD how do you…

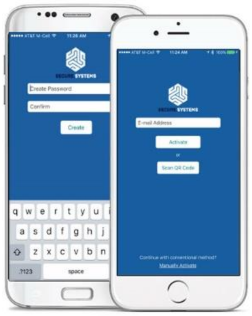
⇒ Enforce Multi Factor Authentication and other password management policies

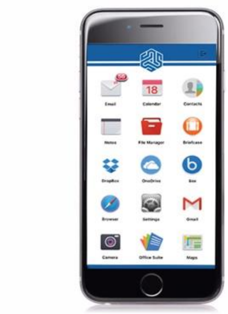
⇒ Ensure the data is protected with FIPS 140-2 / 256 bit encryption - both in transit and at rest

⇒ Enable a guaranteed wipe of all CUI and other work data – without wiping personal data or apps.

⇒ Adhere to ALL Access Control, Identity & Authentication & Info Integrity Controls

The traditional approach of using MDM/EMM solutions has proven time and again to simply NOT be enough. It's focused on the device, not the data, it's more vulnerable to malware and other threats, and it creates a level of distrust between the employees and the company. The less complicated and more secure approach is to use a containerized Workspace. A containerized Workspace creates a seamless and highly secure partition on any iOS or Android device that completely separates business data and applications from personal use information - enabling your employees, and even contractors and other 3rd party workers, to securely access CUI data from any device.





Introducing SyncDog – the next generation solution for mobile enablement. The SyncDog Secure.Systems solution is a full end-to-end mobile security platform offerin MDM, Mobile Threat Defense (MTD), Secure Email and Messaging, and a Containerized Workspace. It leverages multi-factor authentication, biometric and other password management solutions and combines it with Validated FIPS 140-2 256 bit encryption to secure and protect the data– no matter what device it's on. Coporate Owned, BYOD or any combination thereof, is now a reality, and its more secure and easier to implement than the solutions you are currently using. Furthermore, sharing data with contractors and other 3rd party workers is now easier and more secure than it's ever been. And When the time comes that the device or employee no longer needs access to all, or some of the data, it can be easily and assuredly, removed from the device without impacting any of the personal data (pictures, text streams, contact lists etc.) on the device.

Secure.Systems easily integrates into existing endpoint management solutions and can be deployed from the cloud, on-premise or as a hybrid deploymen

SECURE.SYSTEMS

PROTECTED BY SYNCDOG