CMMC 2.0 MOBILITY REQUIREMENTS MATRIX

SYNCDog's Secure.Systems™ is the most complete solution available to enable Defense Industrial Base (DIB) supply chain teams adhere to NIST guidelines to ensure protection of CUI, Federal Contract Information (FCI) and For Official Use Only (FOUO) data on Mobile Devices. SYNCDog's Secure.Systems™ provides a Validated FIPS 140-2 Certified solution that offers DIB suppliers the functionality to meet ALL of the CMMC requirements pertaining to mobile devices for certification at all Levels while future proofing you for ones to come. The following worksheet breaks down each of the 14 domains and highlights all the controls that apply to mobility, and then offers insight into how SyncDog's Trusted Mobile Workspace can help DIB companies easily adhere to those mandates.

CMMC Mobility Requirements Matrix - Table of Contents

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. SYNCDOG INC., MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL NOR ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Access Control (AC)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
AC.L1-3.1.1	1	X	Authorized Access Control	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer system access rights based on the profile and entitlements of that user	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC.1.001	1	3.1.1
AC.L1-3.1.2	1	X	Transaction & Function Control	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer transaction and function rights based on the profile and entitlements of that user	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC.1.002	1	3.1.2
AC.L2-3.1.3	2	X	Control CUI Flow	SyncDog offers out of the box functionality to accurately control the flow of CUI based on the profile and entitlements of the end user, the time of day/week access is allowed as well as the location of the user at the time.	Control the flow of CUI in accordance with approved authorizations.	AC.2.016	2	3.1.3
AC.L2-3.1.4	2	X	Separation of Duties	SyncDog offers out of the box functionality to accurately identify the end user to reduce the risk of malevolent behavior by separating the duties of individuals based on the profile and entitlements of that user.	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC.3.017	3	3.1.4
AC.L2-3.1.5	2	X	Least Privilege	The SyncDog solution was purpose built to easily address the varying needs of differing roles, titles, security functions and privileged accounts from within the admin console. Privileges are are easily established and enforced based on the specific and minimal needs to fulfill the duties of the job all withing a "single plane of glass" where all customers,	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC.2.007	2	3.1.5
AC.L2-3.1.6	2	X	Non-Privileged Account Use	SyncDog creates an environment where multiple accounts can be established on a single mobile device where priveledged vs. non-priviledged data is completely separated with safeguards established to prevent cutting/pasting between those accounts	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC.2.008	2	3.1.6
AC.L2-3.1.7	2	X	Privileged Functions	SyncDog uses profiles and entitlements to identify and administer rights and priviledges of every user. The solution establishes a chain of custody by tracking and auditing all access and usage of data and files, execution of functions, and login and access attempts to the solution itself.	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	AC.3.018	3	3.1.7
AC.L2-3.1.8	2	X	Unsuccessful Logon Attempts	Out of the box functionality	Limit unsuccessful logon attempts.	AC.2.009	2	3.1.8
AC.L2-3.1.9	2	X	Privacy & Security Notices	Out of the box functionality	Provide privacy and security notices consistent with applicable CUI rules.	AC.2.005	2	3.1.9
AC.L2-3.1.10	2	X	Session Lock	Out of the box functionality	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	AC.2.010	2	3.1.10
AC.L2-3.1.11	2	X	Session Termination	Out of the box functionality	Terminate (automatically) user sessions after a defined condition.	AC.3.019	3	3.1.11
AC.L2-3.1.12	2	X	Control Remote Access	Out of the box functionality	Monitor and control remote access sessions.	AC.2.013	2	3.1.12
AC.L2-3.1.13	2	X	Remote Access Confidentiality	SyncDog uses Validated FiPS 140-2 Certified 256 bit encryption to secure all information being accessed through our solution while in transit and while at rest	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC.3.014	3	3.1.13
AC.L2-3.1.14	2	X	Remote Access Routing	Out of the box functionality	Route remote access via managed access control points.	AC.2.015	2	3.1.14
AC.L2-3.1.15	2	X	Privileged Remote Access	SyncDog allows administrators to remotely lock or wipe container data. SyncDog's Trusted Mobile Workspace also supports automatic data wipe "timebomb" policies, and can remotely report on device security vulnerabilities via in-app scanning tools that automatically sync vulnerability data to administrators.	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC.3.021	3	3.1.15
AC.L2-3.1.16	2	X	Wireless Access Authorization	SyncDog's trusted mobile workspace ensures all data that flows over such connections is encrypted at all times effectively removing all concerns about how the device is connecting.	Authorize wireless access prior to allowing such connections.	AC.2.011	2	3.1.16
AC.L2-3.1.17	2	X	Wireless Access Protection	SyncDog's trusted mobile workspace alleviates concerns on how the device is connected by ensuring all data that flows over such connections is encrypted at all times using Validated FiPS Certified 256 bit encryption	Protect wireless access using authentication and encryption.	AC.3.012	3	3.1.17
AC.L2-3.1.18	2	X	Mobile Device Connection	SyncDog's Trusted Mobile Workspace enables fully secure access from mobile devices by using Validated FiPS 140-2 Certified 256 bit enryption while assigning and incorporating profiles and entitlements to identify rights and priviledges of every authorized mobile user.	Control connection of mobile devices.	AC.3.020	3	3.1.18
AC.L2-3.1.19	2	X	Encrypt CUI on Mobile	SyncDog's Trusted Mobile Workspace creates fully secure access from mobile devices and endpoints by using Validated FiPS 140-2 Certified 256 bit enryption while assigning and incorporating profiles and entitlements to identify rights and priviledges of every mobile user. Our Data Loss Protection (DLP) and Data integrity capabilities are the hallmark of our solution.	Encrypt CUI on mobile devices and mobile computing platforms.	AC.3.022	3	3.1.19
AC.L2-3.1.21	2	X	Portable Storage Use	Out of the box functionality	Limit use of portable storage devices on external systems.	AC.2.006	2	3.1.21

Awareness and Training (AT)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
AT.L2-3.2.1	2	X	Role-Based Risk Awareness	SyncDog is easily incorporated in these corporate policies, practices and procedures and even incorporates a Mobile Threat Defense module to continously and autonomously monitor the environment for possible risks	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT.2.056	2	3.2.1
AT.L2-3.2.2	2	X	Role-Based Training	SyncDog is easily incorporated in these corporate policies, practices and procedures	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	AT.2.057	2	3.2.2
AT.L2-3.2.3	2		Insider Threat Awareness		Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT.3.058	3	3.2.3

Audit and Accountability (AU)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
AU.L2-3.3.1	2	X	System Auditing	Out of the box functionality where SyncDog establishes a chain of custody by offering detailed device audit logs and reporting for all user and device activity	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	AU.2.042	2	3.3.1
AU.L2-3.3.2	2	X	User Accountability	Out of the box functionality where SyncDog establishes a chain of custody by offering detailed device audit logs and reporting for all user and device activity	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	AU.2.041	2	3.3.2
AU.L2-3.3.3	2		Event Review		Review and update logged events.	AU.3.045	3	3.3.3
AU.L2-3.3.4	2	X	Audit Failure Alerting	SyncDog provides many system alerts to provide adminsitrators with information on system health or failures	Alert in the event of an audit logging process failure.	AU.3.046	3	3.3.4
AU.L2-3.3.5	2		Audit Correlation		Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	AU.3.051	3	3.3.5
AU.L2-3.3.6	2		Reduction & Reporting	Out of the box functionality where SyncDog establishes a chain of custody by offering detailed device audit logs and reporting for all user and device activity	Provide audit record reduction and report generation to support on-demand analysis and reporting.	AU.3.052	3	3.3.6
AU.L2-3.3.7	2	X	Authoritative Time Source	SyncDog offers a tamper proof time mechanism to prevent manipulation of time stamps and similar annotations	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU.2.043	2	3.3.7
AU.L2-3.3.8	2	X	Audit Protection	Out of the box functionality	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	AU.3.049	3	3.3.8
AU.L2-3.3.9	2		Audit Management	Out of the box functionality	Limit management of audit logging functionality to a subset of privileged users.	AU.3.050	3	3.3.9

Configuration Management (CM)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
CM.L2.3.4.1	2	X	System Baselining	Out of the box functionality	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CM.2.061	2	3.1.1
CM.L2.3.4.2	2	X	Security Configuration Enforcement	SyncDog is easily incorporated into and often exceeds these corporate policies, practices and procedures helping future proof the security architecture	Establish and enforce security configuration settings for information technology products employed in organizational systems.	CM.2.064	2	3.4.2
CM.L2.3.4.3	2	X	System Change Management	SyncDog creates a chain of custody by incorporating logging into all its core components, while also providing support for different user permission levels and a wide variety of policy configurations to control access to organizational systems.	Track, review, approve, or disapprove, and log changes to organizational systems.	CM.2.065	2	3.4.3
CM.L2.3.4.4	2	X	Security Impact Analysis	Policy changes within the SyncDog platform can be easily implemented using staging environment network infrastructure and devices, in order to test implementation impacts prior to live deployment	Analyze the security impact of changes prior to implementation.	CM.2.066	2	3.4.4
CM.L2.3.4.5	2		Acess Restrictions for Change	SyncDog offers a seamless method of mapping organizational structures which can then be used to determine permissions and entitlements - even down to individual users.	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM.2.067	3	3.4.5
CM.L2.3.4.6	2	X	Least Functionality	SyncDog's access management capabilities, based on roles and profiles -even down to the individual user, offers easily managed and granular control of access rights to data, apps and devices	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM.2.062	2	3.4.6
CM.L2.3.4.7	2	X	Nonessential Functionality	SyncDog's access management capabilities, based on roles and profiles -even down to the individual user, offers easily managed and granular control of access rights to data, apps and devices	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	CM.2.068	3	3.4.7
CM.L2.3.4.8	2	X	Application Execution Policy	Out of the box functionality as well as offering a true Zero Trust application workspace that securely separates all work related email, applications and data from all personal use applications effectively negating the need to curtail personal use applications - Secure BYOD is now fully realizable	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	CM.2.069	3	3.4.8
CM.L2.3.4.9	2	X	User Installed Software	Out of the box functionality as well as offering a true Zero Trust application workspace that securely separates all work related email, applications and data from all personal use applications effectively negating the need to curtail personal use applications - Secure BYOD is now fully realizable	Control and monitor user-installed software.	CM.2.063	2	3.4.9

Identification and Authentication (IA)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
IA.L1-3.5.1	1	X	Identification	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer access rights based on the profile and entitlements of that user	Identify information system users, processes acting on behalf of users, or devices.	IA.1.076	1	3.5.1
IA.L1-3.5.2	1	X	Authentication	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer access rights based on the profile and entitlements of that user	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA.1.077	1	3.5.2
IA.L2-3.5.3	2	X	Multifactor Authentication	SyncDog is fully compliant with Out of the Box functionality for both iOS and Android devices	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA.1.083	3	3.5.3
IA.L2-3.5.4	2	X	Replay-Resistant Authentication	Fully Compliant. SyncDog protects against Man-in-the-Middle attacks and SSL replay attacks	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	IA.1.084	3	3.5.4
IA.L2-3.5.5	2	X	Identifier Reuse	SyncDog performs randomized changes to our aes keys with every transaction	Prevent the reuse of identifiers for a defined period.	IA.1.085	3	3.5.5
IA.L2-3.5.6	2		Identifier Handling	SyncDog performs randomized changes to our aes keys with every transaction	Disable identifiers after a defined period of inactivity.	IA.1.086	3	3.5.6
IA.L2-3.5.7	2	X	Password Complexity	SyncDog is fully compliant with Out of the Box functionality	Enforce a minimum password complexity and change of characters when new passwords are created.	IA.1.078	2	3.5.7
IA.L2-3.5.9	2	X	Password Reuse	SyncDog is fully compliant with Out of the Box functionality	Prohibit password reuse for a specified number of generations.	IA.1.079	2	3.5.8
IA.L2-3.5.9	2	X	Temporary Passwords	SyncDog is fully compliant with Out of the Box functionality	Allow temporary password use for system logons with an immediate change to a permanent password.	IA.1.080	2	3.5.9
IA.L2-3.5.10	2	X	Cryptographically-Protected Passwords	SyncDog stores the container password in our encrypted data store, and only transmits data, passwords or otherwise, via our secure encryption	Store and transmit only cryptographically-protected passwords.	IA.1.081	2	3.5.10
IA.L2-3.5.11	2	X	Obscure Feedback	SyncDog's provisioning process uses a FIPS approved algorithm for ECDH key exchange, and after provisioning, container access is a protected by an in-memory process and not subject to observations	Obscure feedback of authentication information.	IA.1.082	2	3.5.1

Incident Response (IR)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
IR.L2-3.6.1	2		Incident Handling		Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	IR.2.092	2	3.6.1
IR.L2-3.6.2	2	X	Incident Reporting	SyncDog's solutions can be set up to automatically notify administrators of detected incidents - configurable down to a per-incident basis.	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	IR.2.098	3	3.6.2
IR.L2-3.6.3	2	X	Incident Response Testing	Test incidents can be simulated using test devices/policy configurations	Test the organizational incident response capability.	IR.2.099	3	3.6.3

Maintenance (MA)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
MA.L2-3.7.1`	2		Perform Maintenance		Perform maintenance on organizational systems.	MA.3.111	2	3.7.1
MA.L2-3.7.2	2		System Maintenance Control		Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA.3.112	2	3.7.2
MA.L2-3.7.3	2		Equipment Sanitization		Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA.3.115	3	3.7.3
MA.L2-3.7.4	2		Media Inspection		Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	MA.3.116	3	3.7.4
MA.L2-3.7.5	2		Nonlocal Maintenance		Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA.3.113	2	3.7.5
MA.L2-3.7.6	2		Maintenance Personnel		Supervise the maintenance activities of personnel without required access authorization.	MA.3.114	2	3.7.6

Media Protection (MP)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
MP.L2-3.8.1	1	X	Media Protection		Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP.2.119	2	3.8.1
MP.L2-3.8.2	1	X	Media Access	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer access rights based on the profile and entitlements of that user	Limit access to CUI on system media to authorized users.	MP.2.120	2	3.8.2
MP.L1-3.8.3	2	X	Media Disposal	SyncDog offers numerouse approaches that GUARANTEES data has been reomved from a devive - even when the device is off-line	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	MP.1.118	1	3.8.3
MP.L2-3.8.4	2	X	Media Markings		Mark media with necessary CUI markings and distribution limitations.	MP.3.122	3	3.8.4
MP.L2-3.8.5	2	X	Media Accountability	SyncDog provides GPS location policies that can control user access to data based on location	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP.3.124	3	3.8.5
MP.L2-3.8.6	2		Portable Storage Encryption	SyncDog is a Validated Fips 140-2 Certified solution that encrypts all data while at Rest and in Transit to only allow access and usage by authorized users	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	MP.3.125	3	3.8.6
MP.L2-3.8.7	2	X	Removable Media		Control the use of removable media on system components.	MP.2.121	2	3.8.7
MP.L2-3.8.8	2	X	Shared Media		Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP.2.123	2	3.8.8
MP.L2-3.8.9	2	X	Protect Backups	SyncDog is fully compliant with Out of the Box functionality	Protect the confidentiality of backup CUI at storage locations.	MP.2.138	2	3.5.9

Personnel Security (PS)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
PS.L2-3.9.1	2		Screen Individuals		Screen individuals prior to authorizing access to organizational systems containing CUI.	PS.2.127	2	3.9.1
PS.L2-3.9.2	2	X	Personnel Actions	SyncDog containers support remote wiping of data and automated deletion of data after a period of time or manually by a simple command. User access to CUI and other work related resources can be strictly controlled by administrators at all times.	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS.2.128	2	3.9.2

Physical Protection (PE)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
PE.L1-3.10.1	1	X	Limit Physical Access	SyncDog offers out of the box functionality to accurately identify the end user and to control and administer access rights based on the profile and entitlements of that user	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	PE.1.131	1	3.10.1
PE.L2-3.10.2	2		Monitor Facility		Protect and monitor the physical facility and support infrastructure for organizational systems.	PE.1.135	2	3.10.2
PE.L1-3.10.3	1		Escort Visitors		Escort visitors and monitor visitor activity.	PE.1.132	1	3.10.3
PE.L1-3.10.4	1		Physical Access Logs		Maintain audit logs of physical access.	PE.1.133	1	3.10.4
PE.L1-3.10.5	1	X	Manage Physical Access	SyncDog utilizes Mobile Device Management technology to inventory, provision and control access to devices through password policy enforcment, access control, device wipe functionality and more. Additionally, SyncDog offers out of the box functionality to accurately identify the end user and to control and administer system access rights based on the profile and entitlements of that user	Control and manage physical access devices.	PE.1.134	1	3.10.5
PE.L2-3.10.6	2		Alternative Work Sites		Enforce safeguarding measures for CUI at alternate work sites.	PE.3.136	3	3.10.6

Risk Assessment (RA)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
RA.L2-3.11.1	2		Risk Assessments		Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	RM.2.141	2	3.11.1
RA.L2-3.11.2	2	X	Vulnerability Scan	SyncDog containers have internal scanning tools that automatically identify threats on the device and support configurable, automated responses to those threats	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RM.2.142	2	3.11.2
PE.L1-3.10.3	2	X	Vulnerability Remediation	SyncDog supports configurable responses to identified threats based on risk level	Remediate vulnerabilities in accordance with risk assessments.	RM.2.143	2	3.11.3

Security Assessment (CA)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
CA.L2-3.12.1	2		Security Control Assessment		Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	CA.2.158	2	3.12.1
CA.L2-3.12.2	2		Plan of Action		Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	CA.2.159	2	3.12.2
CA.L2-3.12.3	2	X	Security Control Monitoring	SyncDog supports automated monitoring of its server and device solutions	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	CA.3.161	3	3.12.3
CA.L2-3.12.4	2		System Security Plan		Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	CA.2.157	2	3.12.4

System and Communications Protection (SC)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
SC.L1-3.13.1	1	X	Boundary Protection	SyncDog's Trusted Workspace uses a private, dedicated connection that fully secures access to data by using Validated FiPS 140-2 Certified 256 bit encryption while assigning, incorporating and administering profiles and entitlements that identifies rights and privileges of every user. Our DLP and Data integrity capabilities are the hallmark of our solution.	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	SC.1.175	1	3.13.1
SC.L1-3.13.2	1	X	Security Engineering	SyncDog's designs and development processes are designed for maximum security implementation.	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	SC.1.180	1	3.13.2
SC.L1-3.13.3	2	X	Role Separation	SyncDog's solution provides user permission segmentation and per-user policy management	Separate user functionality from system management functionality.	SC.1.181	3	3.13.3
SC.L1-3.13.4	2	X	Shared Resource Control	SyncDog's Trusted Mobile Workspace creates fully secure access from mobile devices and endpoints by using Validated FiPS 140-2 Certified 256 bit enryption while assigning and incorporating profiles and entitlements to identify rights and priviledges of every mobile user. Our Data Loss Protection (DLP) and Data integrity capabilities are the hallmark of our solution.	Prevent unauthorized and unintended information transfer via shared system resources.	SC.1.182	3	3.13.4
SC.L1-3.13.5	2	X	Public-Access System Separation	A SyncDog on-premise rdeployment separates device access to internal resources, from the internal network, by not allowing packets to traverse from outside the network to inside the network. SyncDog's unique transport technology is superior to VPN implementations because external devices are not actually connected to the internal network, but rather segmented trhough a transport server.	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	IA.1.076	3	3.13.5
SC.L1-3.13.6	2		Network Communication by Exception	SyncDog's on-premise solutions allow all inbound network trafic to be denied at the firewall level while still allowing permitted access to internal resources for devices secured by our container.	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	IA.1.083	3	3.13.6
SC.L1-3.13.7	2	X	Split Tunneling	SyncDog's Trusted Workspace goes one step further by only allowing a single direction communication to and from our workspace and fully encrypts all data being transmitted through that communication channel. Our DLP and Data integrity capabilities are the hallmark of our solution.	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	IA.1.084	2	3.13.7
SC.L1-3.13.8	2	X	Data in Transit	SyncDog's Trusted Workspace secures all data being accessed, transmitted or stored within the solution by using Validated FiPS 140-2 Certified 256 bit encryption to protect access and usage of CUI. Our DLP and Data integrity capabilities are the hallmark of our solution.	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	IA.1.085	2	3.13.8
SC.L1-3.13.9	2	X	Connections Termination	Out of the Box Functionality	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	IA.1.086	2	3.13.9
SC.L1-3.13.10	2	X	Key Management	The SyncDog Trusted workspace provisions using an Elliptic curve Diffie-Hellman key exchange generated with a SHA-256 hashing algorithm. The multi-part crypto key is NOT stored in the crypto key store and is instead, spread out over the device so it can not be re-generated	Establish and manage cryptographic keys for cryptography employed in organizational systems.	IA.1.087	2	3.13.10
SC.L1-3.13.11	2	X	CUI Encryption	SyncDog is fully compliant with Out of the Box functionality	Employ FIPS-Validated cryptography when used to protect the confidentiality of CUI	IA.1.077	3	3.13.11
SC.L1-3.13.12	2	X	Collaborative Device Control	The SyncDog Trusted Workspace enables admistrative control over all devices accessing the workspace and administers control over what apps and data are allowed to be accessed - allowing greater SECURE usage of mobile devices to access CUI and other sensitive information.	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	IA.1.078	2	3.13.12
SC.L1-3.13.13	2	X	Mobile Code	Out of the Box Functionality	Control and monitor the use of mobile code.	IA.1.088	2	3.13.13
SC.L1-3.13.14	2	X	Voice over Internet Protocol	SyncDog will support this functionality in FY 2023	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	IA.1.089	2	3.13.14
SC.L1-3.13.15	2	X	Communications Authenticity	SyncDog's Trusted Workspace goes one step further by only allowing a single direct communication from our workspace and fully encrypts all data being transmitted through that communication channel. Our DLP and Data integrity capabilities are the hallmark of our solution.	Protect the authenticity of communications sessions.	IA.1.090	2	3.13.15
SC.L1-3.13.16	2	X	Data at Rest	Out of the Box Functionality - SyncDog was built from the ground up to ensure all data being accessed, stored and transmitted to and from mobile devices is highly secure. SyncDog uses Validated FIPS 140-2 Certified 256 bit encryption to protect data at Rest, in Use and in Transit.	Protect the confidentiality of CUI at rest.	IA.1.091	2	3.13.16

System and Information Integrity (SI)

CMMC 2.0 Mapping ID	CMMC 2.0 Level	Applies to Mobility ?	Control Title	SyncDog Compliance	Description	CMMC 1.0 ID	CMMC 1.0 Level	NIST 800-171 Reference Pointers
SI.L1-3.14.1	1		Security Alerts & Advisories		Identify, report, and correct information and information system flaws in a timely manner.	SI.1.210	1	3.14.1
SI.L1-3.14.2	1	X	Malicious Code Protection	The SyncDog Trusted Workspace completely isolates CUI/Government and corporate data from the device and operating system, creating an impenetrable shell that malicious code and other corruptive techniques are not able to access. So even if the device becomes corrupted or malicious code is accessed, CUI data and all other data in the workspace is still in tact and protected. Our DLP and Data integrity capabilities are the hallmark of our solution	Provide protection from malicious code at appropriate locations within organizational information systems.	SI.1.211	1	3.14.2
SI.L1-3.14.3	2	X	Security Alerts & Advisories	The SyncDog Trusted Workspace incorporates Anti Virus and Mobile Threat Detection capapbilities as added security measures. Furthermore, even if corrupt data or files are accessed within the workspace or if the device or operating system is corrupted, all data and files within the workspace will remain in tact and protected. Our DLP and Data integrity capabilities are the hallmark of our solution	Monitor system security alerts and advisories and take action in response.	SI.2.214	2	3.14.3
SI.L1-3.14.4	1	X	Update Malicious Code Protection	The SyncDog Trusted Workspace incorporates Anti Virus and Mobile Threat Detection capapbilities as added security measures. So even if corrupt data or files are accessed within the workspace or if the device or operating system is corrupted, all data and files within the workspace will remain in tact and protected. Our DLP and Data integrity capabilities are the hallmark of our solution	Update malicious code protection mechanisms when new releases are available.	SI.1.212	1	3.14.4
SI.L1-3.14.5	1	X	System & File Scanning	Supported. SyncDog incorporates Mobile Threat Defense technology to continuously scan for malicious activiy. Better still, these security mechanisms are only secondary to the isolation and encryption techniques utilized that protects the itegrity of CUI and all other data even in the presence of malicious code and other threats	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	SI.1.213	1	3.14.5
SI.L1-3.14.6	2		Monitor Communications for Attacks	The SyncDog Trusted Workspace completely isolates CUI/Government and corporate data from the device and operating system, creating an impenetrable shell that maicious code and other corruptive techniques are not able to access. So even if the device becomes corrupted or malicious code is accessed, CUI data and all other data in the workspace is still in tact and protected. Our DLP and Data integrity capabilities are the hallmark of our solution	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI.2.216	2	3.14.6
SI.L1-3.14.7	2	X	Identify Unauthorized Use	SyncDog uses profiles and entitlements to identify and administer the rights and priviledges of every user, and to track and audit all access and usage of data and files and to the solution itself creating a complete chain of custody of all data accessed. Our DLP and Data integrity capabilities are the hallmark of our solution.	Identify unauthorized use of organizational systems.	SI.2.217	2	3.14.7

SYNCDOG

CMMC - 800-171 Mapping Index

Access Control (AC)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
AC.L1-3.1.1	1	Authorized Access Control	3.1.1	AC.1.001	1
AC.L1-3.1.2	1	Transaction & Function Control	3.1.2	AC.1.002	1
AC.L2-3.1.3	2	Control CUI Flow	3.1.3	AC.2.016	2
AC.L2-3.1.4	2	Separation of Duties	3.1.4	AC.3.017	3
AC.L2-3.1.5	2	Least Privilege	3.1.5	AC.2.007	2
AC.L2-3.1.6	2	Non-Privileged Account Use	3.1.6	AC.2.008	2
AC.L2-3.1.7	2	Privileged Functions	3.1.7	AC.3.018	3
AC.L2-3.1.8	2	Unsuccessful Logon Attempts	3.1.8	AC.2.009	2
AC.L2-3.1.9	2	Privacy & Security Notices	3.1.9	AC.2.005	2
AC.L2-3.1.10	2	Session Lock	3.1.10	AC.2.010	2
AC.L2-3.1.11	2	Session Termination	3.1.11	AC.3.019	3
AC.L2-3.1.12	2	Control Remote Access	3.1.12	AC.2.013	2
AC.L2-3.1.13	2	Remote Access Confidentiality	3.1.13	AC.3.014	3
AC.L2-3.1.14	2	Remote Access Routing	3.1.14	AC.2.015	2
AC.L2-3.1.15	2	Privileged Remote Access	3.1.15	AC.3.021	3
AC.L2-3.1.16	2	Wireless Access Authorization	3.1.16	AC.2.011	2
AC.L2-3.1.17	2	Wireless Access Protection	3.1.17	AC.3.012	3
AC.L2-3.1.18	2	Mobile Device Connection	3.1.18	AC.3.020	3
AC.L2-3.1.19	2	Encrypt CUI on Mobile	3.1.19	AC.3.022	3
AC.L2-3.1.21	2	Portable Storage Use	3.1.21	AC.2.006	2

Awareness & Training (AT)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
AT.L2-3.2.1	2	Role-Based Risk Awareness	3.2.1	AT.2.056	2
AT.L2-3.2.2	2	Role-Based Training	3.2.2	AT.2.057	2
AT.L2-3.2.3	2	Insider Threat Awareness	3.2.3	AT.3.058	3

Audit & Accountability (AU)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
AU.L2-3.3.1	2	System Auditing	3.3.1	AU.2.042	2
AU.L2-3.3.2	2	User Accountability	3.3.2	AU.2.041	2
AU.L2-3.3.3	2	Event Review	3.3.3	AU.3.045	3
AU.L2-3.3.4	2	Audit Failure Alerting	3.3.4	AU.3.046	3
AU.L2-3.3.5	2	Audit Correlation	3.3.5	AU.3.051	3
AU.L2-3.3.6	2	Reduction & Reporting	3.3.6	AU.3.052	3
AU.L2-3.3.7	2	Authoritative Time Source	3.3.7	AU.2.043	2
AU.L2-3.3.8	2	Audit Protection	3.3.8	AU.3.049	3
AU.L2-3.3.9	2	Audit Management	3.3.9	AU.3.050	3

Configuration Management (CM)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
CM.L2.3.4.1	2	System Baselining	3.1.1	CM.2.061	2
CM.L2.3.4.2	2	Security Configuration Enforcement	3.4.2	CM.2.064	2
CM.L2.3.4.3	2	System Change Management	3.4.3	CM.2.065	2
CM.L2.3.4.4	2	Security Impact Analysis	3.4.4	CM.2.066	2
CM.L2.3.4.5	2	Acess Restrictions for Change	3.4.5	CM.2.067	3
CM.L2.3.4.6	2	Least Functionality	3.4.6	CM.2.062	2
CM.L2.3.4.7	2	Nonessential Functionality	3.4.7	CM.2.068	3
CM.L2.3.4.8	2	Application Execution Policy	3.4.8	CM.2.069	3
CM.L2.3.4.9	2	User Installed Software	3.4.9	CM.2.063	2

Identification & Authentication (IA)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
IA.L1-3.5.1	1	Identification	3.5.1	IA.1.076	1
IA.L1-3.5.2	1	Authentication	3.5.2	IA.1.077	1
IA.L2-3.5.3	2	Multifactor Authentication	3.5.3	IA.1.083	3
IA.L2-3.5.4	2	Replay-Resistant Authentication	3.5.4	IA.1.084	3
IA.L2-3.5.5	2	Identifier Reuse	3.5.5	IA.1.085	3
IA.L2-3.5.6	2	Identifier Handling	3.5.6	IA.1.086	3
IA.L2-3.5.7	2	Password Complexity	3.5.7	IA.1.078	2
IA.L2-3.5.8	2	Password Reuse	3.5.8	IA.1.079	2
IA.L2-3.5.9	2	Temporary Passwords	3.5.9	IA.1.080	2
IA.L2-3.5.10	2	Cryptographically-Protected Passwords	3.5.10	IA.1.081	2
IA.L2-3.5.11	2	Obscure Feedback	3.5.11	IA.1.082	2

Incident Response (IR)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
IR.L2-3.6.1	2	Incident Handling	3.6.1	IR.2.092	2
IR.L2-3.6.2	2	Incident Reporting	3.6.2	IR.2.098	3
IR.L2-3.6.3	2	Incident Response Testing	3.6.3	IR.2.099	3

Maintenance (MA)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
MA.L2-3.7.1	2	Perform Maintenance	3.7.1	MA.3.111	2
MA.L2-3.7.2	2	System Maintenance Control	3.7.2	MA.3.112	2
MA.L2-3.7.3	2	Equipment Sanitization	3.7.3	MA.3.115	3
MA.L2-3.7.4	2	Media Inspection	3.7.4	MA.3.116	3
MA.L2-3.7.5	2	Nonlocal Maintenance	3.7.5	MA.3.113	2
MA.L2-3.7.6	2	Maintenance Personnel	3.7.6	MA.3.114	2

CMMC - 800-171 Mapping Index

Media Protection (MP)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
MP.L2-3.8.1	1	Media Protection	3.8.1	MP.2.119	2
MP.L2-3.8.2	1	Media Access	3.8.2	MP.2.120	2
MP.L1-3.8.3	2	Media Disposal	3.8.3	MP.1.118	1
MP.L2-3.8.4	2	Media Markings	3.8.4	MP.3.122	3
MP.L2-3.8.5	2	Media Accountability	3.8.5	MP.3.124	3
MP.L2-3.8.6	2	Portable Storage Encryption	3.8.6	MP.3.125	3
MP.L2-3.8.7	2	Removable Media	3.8.7	MP.2.121	2
MP.L2-3.8.8	2	Shared Media	3.8.8	MP.2.123	2
MP.L2-3.8.9	2	Protect Backups	3.5.9	MP.2.138	2

Personnel Security (PS)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
PS.L2-3.9.1	2	Screen Individuals	3.9.1	PS.2.127	2
PS.L2-3.9.2	2	Personnel Actions	3.9.2	PS.2.128	2

Physical Protection (PE)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
PE.L1-3.10.1	1	Limit Physical Access	3.10.1	PE.1.131	1
PE.L2-3.10.2	2	Monitor Facility	3.10.2	PE.1.135	2
PE.L1-3.10.3	1	Escort Visitors	3.10.3	PE.1.132	1
PE.L1-3.10.4	1	Physical Access Logs	3.10.4	PE.1.133	1
PE.L1-3.10.5	1	Manage Physical Access	3.10.5	PE.1.134	1
PE.L2-3.10.6	2	Alternative Work Sites	3.10.6	PE.3.136	3

Risk Assessment (RA)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
RA.L2-3.11.1	2	Risk Assessments	3.11.1	RM.2.141	2
RA.L2-3.11.2	2	Vulnerability Scan	3.11.2	RM.2.142	2
RA.L2-3.11.3	2	Vulnerability Remediation	3.11.3	RM.2.143	2

Security Assessment (CA)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
CA.L2-3.12.1	2	Security Control Assessment	3.12.1	CA.2.158	2
CA.L2-3.12.2	2	Plan of Action	3.12.2	CA.2.159	2
CA.L2-3.12.3	2	Security Control Monitoring	3.12.3	CA.3.161	3
CA.L2-3.12.4	2	System Security Plan	3.12.4	CA.2.157	2

System & Communications Protection (SC)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
SC.L1-3.13.1	1	Boundary Protection	3.13.1	SC.1.175	1
SC.L1-3.13.2	1	Security Engineering	3.13.2	SC.1.180	1
SC.L1-3.13.3	2	Role Separation	3.13.3	SC.1.181	3
SC.L1-3.13.4	2	Shared Resource Control	3.13.4	SC.1.182	3
SC.L1-3.13.5	2	Public-Access System Separation	3.13.5	IA.1.076	3
SC.L1-3.13.6	2	Network Communication by Exception	3.13.6	IA.1.083	3
SC.L1-3.13.7	2	Split Tunneling	3.13.7	IA.1.084	2
SC.L1-3.13.8	2	Data in Transit	3.13.8	IA.1.085	2
SC.L1-3.13.9	2	Connections Termination	3.13.9	IA.1.086	2
SC.L1-3.13.10	2	Key Management	3.13.10	IA.1.087	2
SC.L1-3.13.11	2	CUI Encryption	3.13.11	IA.1.077	2
SC.L1-3.13.12	2	Collaborative Device Control	3.13.12	IA.1.078	2
SC.L1-3.13.13	2	Mobile Code	3.13.13	IA.1.088	2
SC.L1-3.13.14	2	Voice over Internet Protocol	3.13.14	IA.1.089	2
SC.L1-3.13.15	2	Communications Authenticity	3.13.15	IA.1.090	2
SC.L1-3.13.16	2	Data at Rest	3.13.16	IA.1.091	2

System & Information Integrity (SI)

CMMC 2.0 ID #	CMMC 2.0 Level	Control Title	NIST 800-171 Reference #'s	CMMC 1.x ID #	CMMC 1.x Level
SI.L1-3.14.1	1	Security Alerts & Advisories	3.14.1	SI.1.210	1
SI.L1-3.14.2	1	Malicious Code Protection	3.14.2	SI.1.211	1
SI.L1-3.14.3	2	Security Alerts & Advisories	3.14.3	SI.2.214	2
SI.L1-3.14.4	1	Update Malicious Code Protection	3.14.4	SI.1.212	1
SI.L1-3.14.5	1	System & File Scanning	3.14.5	SI.1.213	1
SI.L1-3.14.6	2	Monitor Communications for Attacks	3.14.6	SI.2.216	2
SI.L1-3.14.7	2	Identify Unauthorized Use	3.14.7	SI.2.217	2