KEEPER®

Expedite CMMC with Keeper Security

Keeper enables your organization to protect and prepare for DoD contracts.

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense (DoD) cybersecurity compliance and certification program focused on the independent assessment of defense contractors against NIST 800-171 security controls for protecting Controlled Unclassified Information (CUI).

The Defense Industrial Base (DIB) continues to be a target of hostile nation states because of the sensitive information stored on their corporate networks.

CMMC builds upon the existing DFARS 252.204-7012 regulations. Access controls and data protection are at the forefront of the model to reduce the risk of cyber threats.

A 2019 security audit of ten prime contractors by the Defense Contract Management Agency found that one of the most common security shortfalls was weak passwords. Weak passwords continue to be a cybersecurity gap that fuels an ever-growing threat of compromise and critical data loss to our adversaries.

Meeting CMMC's security controls requires a combination of people, processes and technology. By implementing Keeper Security Government Cloud (KSGC), DoD contractors can address coverage on 26 of the 110 controls in CMMC level 2.

Future Proofing & Going Beyond Checking the Boxes

The majority of CMMC's security controls are based on NIST 800-171 Revision 2, which was released in 2020. NIST 800-171 Revision 3 is being released in the 1st quarter of 2024 and includes new requirements for passwords.

An organization's passwords are its de facto keys to the kingdom, but the current control set in NIST 800-171 Revision 2 does not address the latest secure password management best practices.

A security team usually has little to no visibility into their organization's password security posture. Keeper gives security teams visibility into the strengths and weaknesses of their organizations' passwords and alerts administrators when passwords have been compromised or if users are not complying with organizational password policies, such as prohibitions on password reuse. This allows administrators to proactively address weaknesses and prevent cyber incidents.

CMMC will eventually adopt the 3rd revision of NIST 800-171, and defense contractors will need to account for new requirements such as:

- Changing passwords when they have been compromised.
- Ensuring that new or updated passwords are not on lists of commonly used, expected or compromised passwords.

Definitions:

- Meets - Keeper can be used as a primary means to **satisfy** a security control in your System Security Plan (SSP).
- Supports - Keeper can be used to **strengthen the posture** of a security control in your SSP.

Security Control	Security Control Title	Status	Comments
AC.L2-3.1.1	Authorized Access Control (CUI)	Supports	Keeper's Enterprise Password Manager (EPM) allows users to generate and store secure and unique passwords that support user authentication.
AC.L2-3.1.11	Session Termination	Supports	Keeper provides platform-specific session termination controls based on a period of time. EPM also provides re-authentication options for actions like autofilling a password.
AC.L2-3.1.12	Control Remote Access	Meets	KCM is a remote access gateway used to grant users access to resources in accordance with least privilege principles. It uses connection protocols such as RDP, HTTPS, SSH, VNC, Telnet, Kubernetes, MySQL, PostgreSQL, and SQL.
AC.L2-3.1.13	Remote Access Confidentiality	Meets	KCM uses FIPS 140-2 validated encryption to ensure remote access confidentiality.
AC.L2-3.1.14	Remote Access Routing	Meets	KCM is a remote access gateway which serves as a managed access control point.
AC.L2-3.1.15	Privileged Remote Access	Meets	KCM can limit user access to specific connections, limit access to a specific application within an RDP session and limit access by automatically running SSH commands at connection.
AU.L2-3.3.1	System Auditing	Supports	Keeper's Advanced Reporting and Alerts Module (ARAM) provides enterprise level auditing and reporting of admin and user activity.
AU.L2-3.3.5	Audit Correlation	Supports	Keeper's ARAM seamlessly integrates with SIEM solutions for long-term storage and audit correlation.
AU.L2-3.3.6	Reduction & Reporting	Supports	Keeper's ARAM provides filters for 200+ event types.

Security Control	Security Control Title	Status	Comments
CM.L2-3.4.2	Security Configuration Enforcement	Supports	EPM offers extensive group-based policies that control how Keeper can be used.
CM.L2-3.4.6	Least Functionality	Supports	KCM can limit a remote RDP session to a single application, control clipboard behavior, disable printing and more.
IA.L2-3.5.10	Cryptographically Protected Passwords	Meets	EPM securely stores and transmits passwords using FIPS 140-2 validated encryption.
IA.L2-3.5.11	Obscure Feedback	Supports	EPM masks passwords and other sensitive information. Keeper also allows for the creation of custom record types with masking settings for each custom field.
IA.L2-3.5.3	Multi-Factor Authentication	Supports	Keeper supports multiple MFA methods including TOTP, RSA SecureID, Duo Security, FIDO2 security keys, Windows Hello and mobile device biometric authentication. It also requires additional approval when a new device is used to access an account.
IA.L2-3.5.4	Replay-Resistant Authentication	Meets	KSM transmits secrets in an encrypted TLS tunnel. The secrets are decrypted by the user's device.
IA.L2-3.5.7	Password Complexity	Meets	EPM offers customizable password complexity settings for master passwords, and passwords generated for defined domains and IP addresses. Security audit reports show stats on the strengths and weaknesses of passwords in the organization.
IA.L2-3.5.8	Password Reuse	Meets	EPM enables organizations to eliminate password reuse by generating unique passwords for every account. Security audit reports show password reuse statistics.
IA.L2-3.5.9	Temporary Passwords	Supports	EPM allows for secure sharing of temporary credentials by transferring ownership of a password record or through a one-time share.

Security Control	Security Control Title	Status	Comments
SC.L2-3.13.10	Key Management	Supports	KSM securely stores and transmits secrets such as SSH keys, API keys, encryption keys, passwords and more using FIPS 140-2 validated zero-knowledge encryption. KSM can also automatically rotate secrets.
SC.L2-3.13.11	CUI Encryption	Meets	EPM uses its FIPS 140-2 validated zero-knowledge encryption to encrypt any CUI and is FedRAMP Authorized at the Moderate Impact level.
SC.L2-3.13.16	Data at Rest	Meets	EPM uses FIPS 140-2 validated zero-knowledge encryption to encrypt any CUI stored in the system at rest and is FedRAMP Authorized at the Moderate Impact level.
SC.L2-3.13.6	Network Communication by Exception	Supports	Network access can be restricted by enabling IP address allow listing.
SC.L2-3.13.8	Data in Transit	Meets	EPM uses FIPS 140-2 validated zero-knowledge encryption to encrypt any CUI in transit and is FedRAMP Authorized at the Moderate Impact level.
SC.L2-3.13.9	Connections Termination	Meets	KCM session timeout settings are configurable.
SI.L2-3.14.3	Security Alerts & Advisories	Supports	Keeper's BreachWatch monitors passwords for indicators of compromise and alerts the user or admin if any of the passwords have been impacted in a breach.
SI.L2-3.14.7	Identify Unauthorized Use	Supports	Keeper's ARAM allows for the creation of alerts based on 200+ event types. EPM's Compliance Reporting module provides additional reporting to identify unauthorized sharing or use of passwords.

KSGC provides a comprehensive CMMC package that includes documentation for the controls on password compliance and how DoD contractors can achieve CMMC certification by implementing Keeper's Enterprise Password Management platform with reporting capabilities.

Keeper Addresses Your CMMC Requirements

KSGC seamlessly integrates into your DoD contract requirements by addressing CMMC password security controls. As a password manager and privileged access manager that is FedRAMP Authorized at the Moderate Impact level, KSGC brings human-centric cybersecurity to the federal government. Using a security platform such as KSGC allows contractors to enforce and require adoption of password security and access management best practices.

FedRAMP

FIPS 140-2

AWS GovCloud

Protect Passwords and Credentials

Keeper's unique security architecture protects data and systems with a solution that is quick to deploy and easy to use. Securely store, share and manage passwords across the entire organization.

Enable Secure Sharing

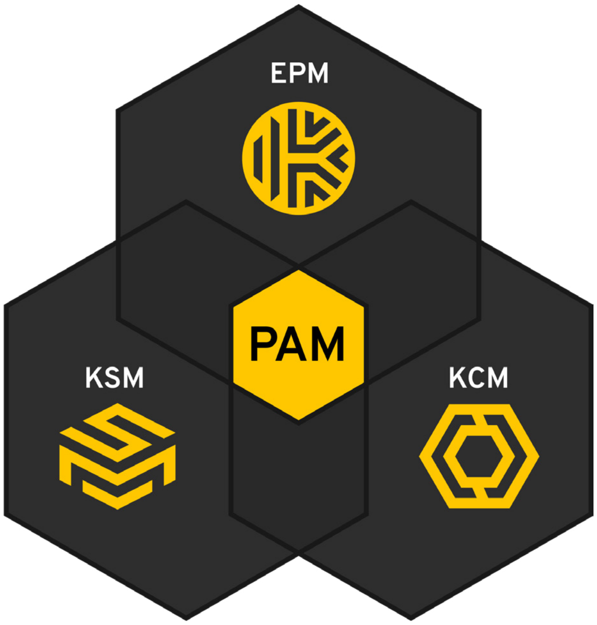
Securely store, share and manage passwords across the entire organization.

Simplify Secure Remote Access

Securely manage your remote connections from anywhere – no VPN required.

Streamline Compliance and Audits

Provide on-demand visibility of access permissions to your organization's credentials and secrets.



KEEPER PASSWORD MANAGER

Enables organizations to securely manage, protect, discover, share and rotate passwords and passkeys with full control and visibility to simplify auditing and compliance.

KEEPER SECRETS MANAGER

Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

KEEPER CONNECTION MANAGER

Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access with RDP, SSH keys, database and Kubernetes endpoints – without the need for a VPN.