KEEPER
Cybersecurity Starts Here™

# Expedite CMMC with Keeper Security

**Keeper Security enables your organization to protect and prepare for DoD Contracts in the most effective and efficient way.**

Meeting CMMC controls requires a team of experts with experience in execution and security to ensure compliance. CMMC has 17 domains with 171 controls that are now essential for DoD contractors moving forward. Keeper Security can help federal contractors address CMMC controls immediately.

During the 2019 security audit of 10 prime contractors by the Defense Contract Management Agency, one of the most common security shortfalls was weak passwords. Weak passwords continue to be a cybersecurity gap that leads to the ever-growing threat of ransomware attacks.

CMMC builds upon existing regulation (DFARS 252.204-7012) and access and data protection and password compliance is at the forefront to reduce risk against cyberthreats.

### CMMC Password Controls Require Enforcement and Reporting

DoD contractors are required to implement 171 controls covering 17 domains including, without limitation, asset management, auditing, accountability, planning, security and internal controls. By implementing Keeper Security Government Cloud (KSGC), DoD contractors immediately achieve coverage on 53 of 171 controls.

DoD contractors need more than a policy provided by an IDP. Enterprise Password Management that enforces password best practices is required to address the password controls within CMMC.

| DOMAIN | CAPACITY | PRACTICE |
|---|---|---|
| **Access Control (AC)** | **C001**<br>Establish system access requirements | • Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).<br>• Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.<br>• Limit use of portable storage devices on external systems. |
| | **C002**<br>Control internal system access | • Limit information system access to the types of transactions and functions that authorized users are permitted to execute.<br>• Employ the principle of least privilege, including for specific security functions and privileged accounts.<br>• Limit unsuccessful logon attempts.<br>• Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.<br>• Protect wireless access using authentication and encryption.<br>• Separate the duties of individuals to reduce the risk of malevolent activity without collusion.<br>• Terminate (automatically) user sessions after a defined condition.<br>• Control connection of mobile devices.<br>• Control information flows between security domains on connected systems.<br>• Periodically review and update CUI program access permissions. |

| DOMAIN | CAPACITY | PRACTICE |
|---|---|---|
| **Access Control (AC)** | **C003**<br>Control remote system access | • Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.<br>• Restrict remote network access based on organizational defined risk factors such as time of day, location of access, physical location, network connection state and measured properties of the current user and role. |
| | **C004**<br>Limit data access to authorized users and processes | • Verify and control/limit connections to and use of external information systems.<br>• Control information posted or processed on publicly accessible information systems.<br>• Control the flow of CUI in accordance with approved authorizations.<br>• Encrypt CUI on mobile devices and mobile computing platforms. |
| **Audit & Accountability (AU)** | **C007**<br>Define audit requirements | • Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.<br>• Review and update logged events. |
| | **C008**<br>Perform auditing | • 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.<br>• Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.<br>• Collect audit information (e.g., logs) into one or more central repositories.<br>• Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging. |
| | **C009**<br>Identify and protect audit information | • Protect audit information and audit logging tools from unauthorized access, modification and deletion.<br>• Limit management of audit logging functionality to a subset of privileged users. |
| | **C010**<br>Review and manage audit logs | • Review audit logs.<br>• Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.<br>• Provide audit record reduction and report generation to support on-demand analysis and reporting.<br>• Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally-defined suspicious activity.<br>• Review audit information for broad activity in addition to per-machine activity. |
| **Configuration Management (CM)** | **C013**<br>Establish configuration baselines | • Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. |

| DOMAIN | CAPACITY | PRACTICE |
|---|---|---|
| **Identification & Authentication (IA)** | **C015**<br>Grant access to authenticated entities | • Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.<br>• Enforce a minimum password complexity and change of characters when new passwords are created.<br>• Prohibit password reuse for a specified number of generations.<br>• Allow temporary password use for system logons with an immediate change to a permanent password.<br>• Store and transmit only cryptographically- protected passwords.<br>• Obscure feedback of authentication information.<br>• Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.<br>• Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.<br>• Prevent the reuse of identifiers for a defined period.<br>• Disable identifiers after a defined period of inactivity. |
| **Incident Response (IR)** | **C017**<br>Detect and report events | • Detect and report events. |
| | **C018**<br>Develop and implement a response to a declared incident | • Establish and maintain a Cyber Incident Response Team (CIRT) that can investigate an issue physically or virtually at any location within 24 hours. |
| | **C019**<br>Perform post incident reviews | • Perform root cause analysis on incidents to determine underlying causes. |
| | **C020**<br>Test incident response | • Test the organizational incident response capability.<br>• Perform unannounced operational exercises to demonstrate technical and procedural responses. |
| **Recovery (RE)** | **C029**<br>Manage back-ups | • Regularly perform and test data back-ups.<br>• Protect the confidentiality of backup CUI at storage locations.<br>• Regularly perform complete, comprehensive and resilient data backups as organizationally-defined. |
| | **C030**<br>Manage information security continuity | • Ensure information processing facilities meet organizationally-defined information security continuity, redundancy and availability requirements. |
| **System & Communications Protection (SC)** | **C038**<br>Define security requirements for systems and communications | • Protect the confidentiality of CUI at rest. |

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 this Enterprise Password Management Platform with reporting capabilities.

## Keeper Addresses your CMMC Certification Needs

Keeper Security Government Cloud (KSGC) seamlessly integrates into your DoD contract requirements by addressing CMMC password security controls. As the only password management solution provider available on FedRAMP Marketplace, KSGC brings human-centric cybersecurity to the Federal Government. Enforcing and requiring adoption of password security best practices will secure contractors with access to Controlled Unclassified Information (CUI).

## Keeper Enterprise Protects the Public Sector from the Most Common Cyberattacks

- **Protects Your Organization Against Ransomware Attacks**
  Keeper protects your organization against ransomware attacks using robust administration, controls and visibility over strong password security and real-time dark web monitoring.
- **Mitigate Risk of Data Breaches**
  Keeper uses a zero-trust and zero-knowledge security architecture that provides visibility and control over the organization's password security, with full end-to-end encryption.
- **Reduce Help Desk Costs Related to Password Resets**
  Keeper frees up IT resources by allowing them to focus on mission-critical priorities rather than reacting to help-desk related incidents.
- **Provide Password Security and Protection Across the Entire Organization**
  Every employee on every device gets a private, encrypted vault for storing and managing their passwords, credentials, files and other sensitive data.
- **Prevent Employees from Entering Credentials on Malicious Sites**
  Keeper alerts users on non-compliant websites to mitigate the risk of a phishing attack.
- **Eliminate SSO Security Gaps**
  Keeper SSO Connect® enables organizations to enhance and extend their SSO deployments with an integrated, zero-knowledge password security and encryption solution.
- **Simplify and Strengthen Audit Compliance**
  Keeper supports RBAC, 2FA, auditing, event reporting and compliance with NIST 800-63B, FITARA, CMMC, HIPAA, DPA, FINRA, SOX, SOC 2 (Type 1 and 2), ISO 27001, ITAR and more.
- **FIPS 140-2 Encryption**
  Keeper utilizes validated FIPS 140-2 encryption modules to address rigorous government standards.
- **AWS GovCloud**
  Government organizations can utilize Keeper Enterprise Password Management (EPM) Platform on AWS GovCloud.

## About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-trust, zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage, advanced reporting and messaging. Named PC Magazine's Best Password Manager & Editors' Choice and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award, Keeper is trusted by millions of people and thousands of organizations to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 (Type 1 and 2) and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects organizations of all sizes across every major industry sector.