

# GateKeeper CMMC Compliance Matrix

## PURPOSE

This document is meant to provide the defense industrial base (DIB) with a high-level overview of CMMC requirements and how the GateKeeper platform can help them reach specific levels of compliance.

## BACKGROUND

To strengthen defense industrial base (DIB) cybersecurity and better safeguard Department of Defense (DoD) information, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess existing DoD cybersecurity requirements.

The program provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information.

## Key aspects of the CMMC

**Tiered Model:** CMMC requires companies handling sensitive unclassified DoD information to implement progressively advanced cybersecurity standards based on the information's type and sensitivity, and mandates that these protections flow down to subcontractors.

**Assessment Requirement:** CMMC assessments allow the DoD to verify DIB implementation of existing cybersecurity standards.

**Implementation through Contracts:** DoD contractors and subcontractors handling sensitive unclassified DoD information must achieve a specific CMMC level as a condition of contract award.

## CMMC ASSESSMENT LEVELS

**CMMC Level 1** – Focuses on basic cyber hygiene as the entry-level certification, requiring contractors to implement 17 practices that protect Federal Contract Information (FCI), including password policies, physical access controls, and regular updates. Level 1 suits

organizations handling less sensitive data that do not process Controlled Unclassified Information (CUI).

**CMMC Level 2** – Applies to Controlled Unclassified Information (CUI), requiring compliance with 110 NIST 800-171 controls and either annual self-assessments or third-party assessments every three years depending on sensitivity.

**CMMC Level 3** – The most advanced cybersecurity tier for DoD contractors, focusing on protecting the most sensitive Controlled Unclassified Information (CUI) from Advanced Persistent Threats (APTs). Built on the CMMC Final Level 2, it requires a third-party assessment every three years and an annual affirmation to verify ongoing compliance.

## CMMC DOMAINS COVERED BY GATEKEEPER

The CMMC model consists of 14 domains that align with the families specified in NIST 900-171.

**Access Control** – Requires organizations to restrict system access to authorized users, enforce least privilege, monitor and protect remote and mobile access, and safeguard CUI across sessions, devices, and networks.

**Audit and Accountability** – Requires organizations to create, protect, and review audit logs to monitor user actions, detect unauthorized activity, ensure accountability, and support timely analysis and reporting.

**Identification and Authentication** – Requires organizations to verify users, processes, and devices through multifactor and cryptographically protected methods, enforce strong and non-reusable credentials, and manage identifiers securely to prevent unauthorized access.



**Control Family:**

ACCESS CONTROL (AC)

**Control ID:**

AC-06 03.01.05 (a)

**CMMC Level:** 1**Description**

Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

**GateKeeper Proximity Enterprise**

Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.

**Control Family:**

ACCESS CONTROL (AC)

**Control ID:**

AC-06 03.01.05 (b)

**CMMC Level:** 1**Description**

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

**GateKeeper Proximity Enterprise**

Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.

**Control Family:**

ACCESS CONTROL (AC)

**Control ID:**

AC-06 03.01.05 (c)

**CMMC Level:** 1**Description**

Verify and control/limit connections to and use of external information systems.

**GateKeeper Proximity Enterprise**

Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.



**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-06(05) 03.01.06

**CMMC Level:** 2

**Description**  
Employ the principle of least privilege, including for specific security functions and privileged accounts.

**GateKeeper Proximity Enterprise**  
Provides proximity-based authentication and authorization to workstations. Using GateKeeper, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.

**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-07 03.01.08 (a)

**CMMC Level:** 2

**Description**  
Enforce a limit of consecutive invalid logon attempts.

**GateKeeper Proximity Enterprise**  
Has the ability to lock a user's account after an administrator-defined number of unsuccessful login attempts.

**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-11(01) 03.01.10

**CMMC Level:** 2

**Description**  
Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

**GateKeeper Proximity Enterprise**  
Automatically locks a user's workstation when they are no longer in proximity to their workstation - preventing access/viewing of data.

**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-17(04) 03.01.12

**CMMC Level:** 2

**Description**  
Establish, monitor, and control usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

**GateKeeper Proximity Enterprise**  
Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.



**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-05 03.01.04

**CMMC Level:** 2

**Description**  
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

**GateKeeper Proximity Enterprise**  
Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation, immediately protecting unauthorized users from accessing a system.

**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-06(09) 03.01.07

**CMMC Level:** 2

**Description**  
Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

**GateKeeper Proximity Enterprise**  
Provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, organizations can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.

**Control Family:**  
ACCESS CONTROL (AC)

**Control ID:**  
AC-12 03.01.11

**CMMC Level:** 2

**Description**  
Terminate (automatically) user sessions after a defined condition.

**GateKeeper Proximity Enterprise**  
Automatically locks a user's workstation when they are no longer in proximity to their workstation - preventing access/viewing of data.

**Control Family:**  
AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**  
AU-03 03.03.02

**CMMC Level:** 2

**Description**  
Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

**GateKeeper Proximity Enterprise**  
Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared accounts.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-02 03.03.01 (a)

**CMMC Level:** 2

**Description**

Create audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared accounts. These audit logs are retained indefinitely and can be on on-premise.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-02 03.03.01 (b)

**CMMC Level:** 2

**Description**

Review and update logged events.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-09 03.03.08 (a)

**CMMC Level:** 2

**Description**

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-09(04) 03.03.08 (b)

**CMMC Level:** 2

**Description**

Limit management of audit logging functionality to a subset of privileged users.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-06 03.03.05

**CMMC Level:** 2**Description**

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.

**Control Family:**

AUDIT AND  
ACCOUNTABILITY (AU)

**Control ID:**

AU-07 03.03.06

**CMMC Level:** 2**Description**

Provide audit record reduction and report generation to support on- demand analysis and reporting.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.

**Control Family:**

IDENTIFICATION AND  
AUTHENTICATION (IA)

**Control ID:**

IA-02 03.05.01

**CMMC Level:** 1**Description**

Identify information system users, processes acting on behalf of users, or devices.

**GateKeeper Proximity Enterprise**

Provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it, even on shared computers. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture.

Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-03 03.05.02

**CMMC Level:** 1

**Description**

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

**GateKeeper Proximity Enterprise**

Provides proximity-based identification, authentication, and authorization to workstations. Using GateKeeper Enterprise, an organization can granularly assign access permissions to individuals/groups on a per workstation basis.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-05(01) 03.05.07 (d, e, f)

**CMMC Level:** 2

**Description**

Enforce a minimum password complexity and change of characters when new passwords are created.

**GateKeeper Proximity Enterprise**

Can integrate with an organization's Active Directory to enforce this control.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-05(01) 03.05.07 (a, b)

**CMMC Level:** 2

**Description**

Prohibit password reuse for a specified number of generations.

**GateKeeper Proximity Enterprise**

Can integrate with an organization's Active Directory to enforce this control.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-05(01) 03.05.07 (e)

**CMMC Level:** 2

**Description**

Allow temporary password use for system logons with an immediate change to a permanent password.

**GateKeeper Proximity Enterprise**

Can integrate with an organization's Active Directory to enforce this control.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-06 03.05.11

**CMMC Level:** 2

**Description**

Obscure feedback of authentication information.

**GateKeeper Proximity Enterprise**

PIN login is obscured and all authentication information is obscured.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-02(01,02) 03.05.03

**CMMC Level:** 2

**Description**

Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.

**GateKeeper Proximity Enterprise**

Has the capability to enforce multifactor authentication (MFA) for all access to a workstation.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-02(08) 03.05.04

**CMMC Level:** 2

**Description**

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

**GateKeeper Proximity Enterprise**

Is a proximity-based identification and authentication solution. A user must be present with their physical token to unlock their workstation, making it inherently replay-resistant.

**Control Family:**

IDENTIFICATION AND AUTHENTICATION (IA)

**Control ID:**

IA-04 03.05.05 (c)

**CMMC Level:** 2

**Description**

Prevent the reuse of identifiers after a defined period of inactivity.

**GateKeeper Proximity Enterprise**

Can integrate with an organization's Active Directory to enforce this control.