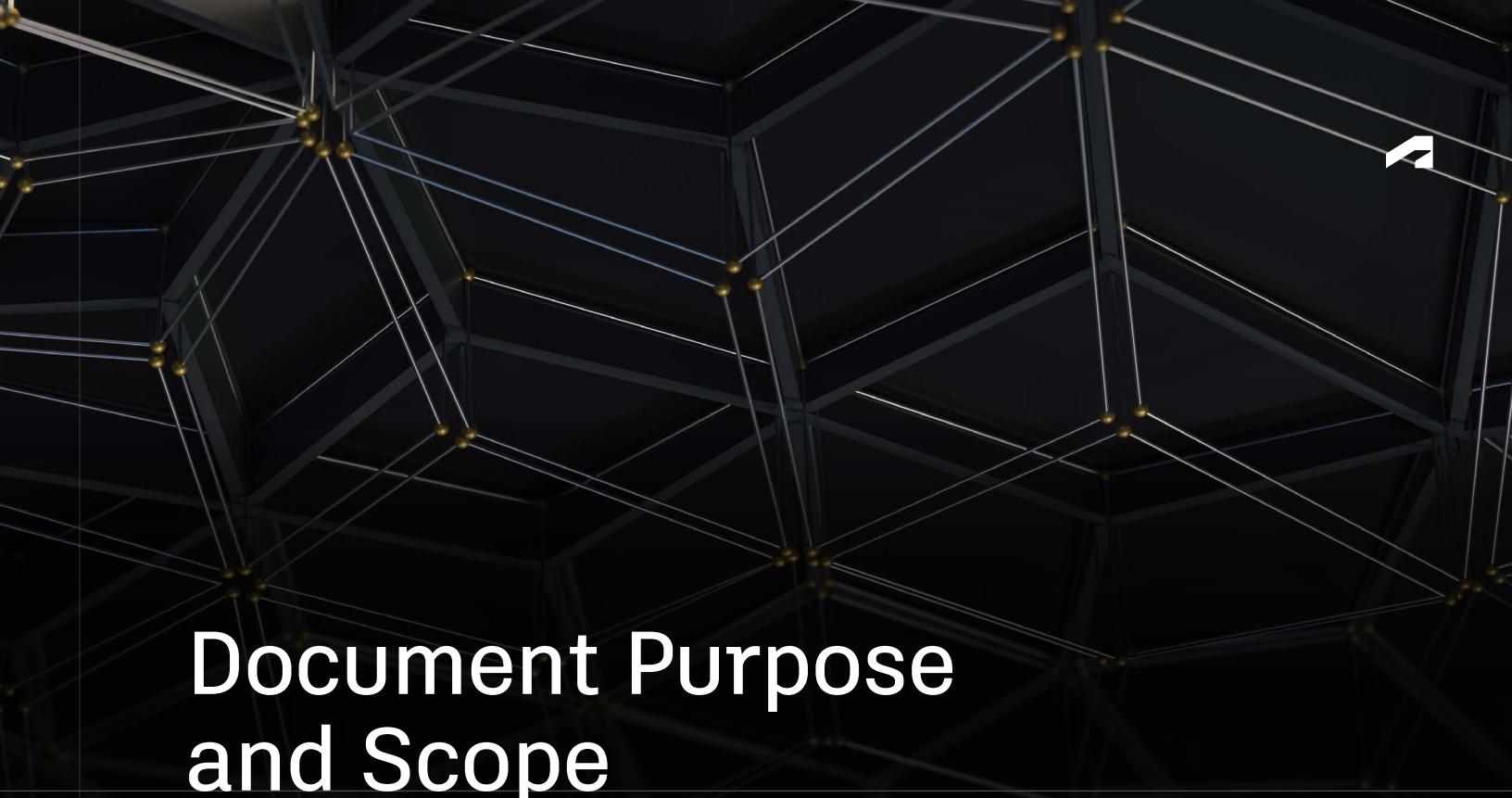
AUTODESK

Cybersecurity Maturity Model Certification Whitepaper

Introduction

The Cybersecurity Maturity Model Certification (CMMC) Program is a regulatory program developed by the United States Department of Defense (DoD) to assess and strengthen the cybersecurity practices of DoD's contractors and subcontractors. CMMC is designed to evaluate the protection of sensitive unclassified information shared by DoD with their vendors and to increase DoD assurance that this data is safeguarded at the appropriate level. Compliance with CMMC will be a requirement for companies that plan to work with the DoD.



Document Purpose and Scope

Autodesk customers that are contractors or subcontractors for the US Department of Defense (DoD) may need to comply with a specific level of CMMC. This document has been created to assist Autodesk customers during their CMMC assessments. It broadly outlines the differences between CMMC levels, with a primary focus on CMMC Level 2. Additionally, it explains the overlap between CMMC and FedRAMP, and provides information about Autodesk offerings available to companies that may have CMMC compliance requirements.

What is included

This whitepaper covers general information about CMMC, an overview of CMMC levels, and the obligations required by CMMC Level 2. It also highlights the differences between FedRAMP and CMMC, and identifies Autodesk products that can be used by DoD contractors and subcontractors.

What is excluded

This whitepaper focuses on CMMC Level 2 and does not include detailed information about CMMC Levels 1 and 3.

Important Notes

- Autodesk has not undergone a CMMC Level 2 assessment and is not currently subject to CMMC Level 2 compliance.
- Autodesk customers are responsible for reviewing the relevant regulations and Autodesk offerings prior to determining which offering best supports their CMMC obligations.
- This document outlines the operations, processes, and security measures implemented by Autodesk to safeguard customers' data within Autodesk's environment only. Autodesk does not assess or certify the security of customer-owned systems, data outside our control, or customer CMMC compliance status.
- Cloud Service offerings not included in Autodesk for Government are outside of the scope of this document.
- No part of this document amends or supersedes any provision of the Autodesk's Terms of Use or other agreements between Autodesk and its customers.
- This whitepaper is based on information generally available as of the date of its publication.

CMMC

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) Program is a regulatory initiative developed and enforced by the United States Department of Defense (DoD). The CMMC Program was created to assess and enhance the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared by the DoD with its contractors and subcontractors, often referred to as the Defense Industrial Base (DIB).

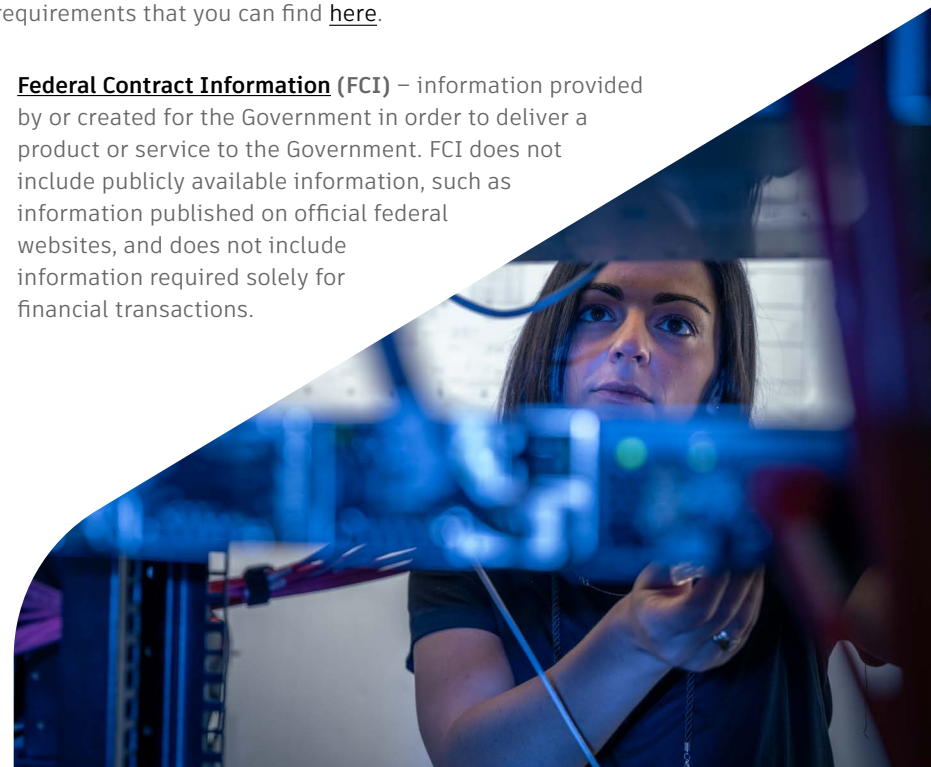
The security requirements for protecting this information already existed before CMMC. They are defined in DFARS clause 252.204–7012, which lists specific security measures that DoD contractors handling FCI or CUI must implement. CMMC does not introduce new security requirements beyond what already exists in the clause. Instead, the key change caused by CMMC is that it now requires DoD contractors to formally validate and demonstrate to DoD that they meet these existing security requirements.

CMMC Levels

There are three levels of CMMC compliance.

CMMC Level 1 focuses on the basic protection of Federal Contract Information (FCI). CMMC Level 1 includes 15 basic safeguarding requirements that you can find here.

> **Federal Contract Information (FCI)** – information provided by or created for the Government in order to deliver a product or service to the Government. FCI does not include publicly available information, such as information published on official federal websites, and does not include information required solely for financial transactions.



CMMC

CMMC Level 2 focuses on the broad protection of Controlled Unclassified Information (CUI). CMMC Level 2 incorporates 110 security requirements listed in NIST SP 800-171 Revision 2*.

> **Controlled Unclassified Information (CUI)** – sensitive information created or owned by the Government. This information is not publicly available and is not classified as "Top Secret", "Secret", or "Confidential". Though CUI is not classified, it must still be protected by companies entrusted with it in accordance with laws, regulations, and policies issued by the Government. CUI is more sensitive than FCI

CMMC Level 3 focuses on a higher level of CUI protection. CMMC Level 3 requires 134 security controls: 110 controls listed in NIST SP 800-171 Revision 2* and 24 controls listed in NIST SP 800-172. These controls are created to protect critical to national security DoD programs or high-value assets that are potential targets for the advanced persistent threat.

According to the DoD's determination, most of its contractors and subcontractors are subject to CMMC Level 1 (63%) or CMMC Level 2 (35%). In this document, we will focus on CMMC Level 2.

*DoD contractors must continue following NIST SP 800-171 Revision 2 for CMMC compliance until the DoD completes transition to Revision 3, according to the Class Deviation issued by DoD on May 2, 2024.

CMMC Model	MODEL	ASSESSMENT
LEVEL 3	134 requirements (110 from NIST SP 800-171 R2* plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	110 requirements listed in NIST SP 800-171 R2*	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	15 requirements listed in FAR 52.204-21	• Annual self-assessment • Annual Affirmation

CMMC

CMMC Level 2

CMMC Level 2 specifies the requirements that must be followed by DoD contractors or subcontractors entrusted with Controlled Unclassified Information (CUI).

CMMC Level 2 compliance focuses on the broad protection of CUI and includes guidance and compliance with several different resources, including:

- Safeguarding Covered Defense Information and Cyber Incident Reporting; DFARS clause 252.204–7012
- Protecting CUI in Nonfederal Systems; NIST SP 800-171
- CMMC Program rule; 32 CFR part 170
- CMMC Acquisition rule; 48 CFR part 204

We will cover some of the main points specified in these resources.

> **Covered defense information (CDI) -** controlled unclassified technical or other information created or owned by DoD. This information can be provided by or on behalf of DoD to a contractor, or it can be produced by a contractor while delivering requested services. CDI requires specific safeguarding or dissemination controls as determined by Government policies, laws, and regulations.

Safeguarding Covered Defense Information and Cyber Incident Reporting, or DFARS clause 252.204–7012

DFARS clause 252.204-7012 applies to defense contractors that handle Covered Defense Information (CDI). Under this clause, contractors must implement specific cybersecurity requirements on any contractor-owned or operated systems that process, store, or transmit CDI.

The DFARS clause also includes some additional requirements, most notably:

1. Defense contractors are required to provide adequate security on all their information systems. To achieve this, they have to implement 110 security requirements specified in "NIST SP 800–171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

CMMC

2. Defense contractors must confirm that any Cloud Service Providers (CSPs) used by them to handle CUI are Federal Risk and Authorization Management Program (FedRAMP®) Moderate Authorized or meet equivalent requirements.

Cloud Service Offering (CSO) must either be FedRAMP® Moderate Authorized or equivalent. Contractors can leverage FedRAMP Moderate Authorized Cloud Service Offerings without assessing whether a CSO meets equivalency requirements. Autodesk for Government offering is FedRAMP Moderate Authorized and, as such, serves as an example of a CSO that does not require additional assessments.

3. All subcontractors that will process, store, or transmit CUI shared with a Defense contractor must follow the same requirements as the contractor itself. Contractor needs to ensure that their subcontractors are protecting CUI at the same level as they do.

4. It is the DoD's responsibility to mark CDI or identify it in some other way in the contract with the DoD vendor. DoD also needs to specify marking requirements for CDI created by the contractor during service delivery.

5. If there is a cybersecurity incident that affects systems containing CDI, defense contractors must report it to DoD within 72 hours of discovery using the process outlined in the DFARS clause.

External Service Provider (ESP) that is a Cloud Service Provider (CSP) – a cloud service vendor that provides a platform, infrastructure, applications, and/or storage on the cloud to its clients.

Controlled technical information (CTI) – technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

CMMC

CMMC Program Rule, or 32 CFR part 170

The CMMC Program rule establishes the CMMC Program and defines general requirements for DoD contractors and subcontractors that handle FCI or CUI, as well as controls specific to the CMMC level required by the contract.

The CMMC Program rule builds upon DFARS 252.204-7012 by establishing a tiered model, assessment requirements, and phased implementation. The DFARS clause requires contractors to implement security controls. The CMMC adds a validation step – contractors must confirm they meet the security requirements outlined in the DFARS clause.

CMMC Acquisition Rule, or 48 CFR part 204

The CMMC Acquisition Rule allows the Department of Defense to require a specific CMMC level in a solicitation* or contract with DoD contractors and subcontractors. The rule was published on September 10, 2025, and becomes effective on November 10, 2025 – exactly 60 days later. Beginning November 10, DoD will start the first phase of CMMC implementation, with additional requirements rolling out over the following years.

*Solicitation – a formal request from the Government sent out when they want to hire contractors.
**In some contracts, DoD may require compliance with CMMC in advance of the planned phase. For example, they may require CMMC Level 2 verified by a CMMC third-party assessment organization before Phase 2.

FedRAMP® vs. CMMC

KEY DIFFERENCES BETWEEN CMMC AND FEDRAMP

DECISION TREE

Both FedRAMP and CMMC are programs developed by the United States Government to standardize the assessment and security requirements for the protection and safeguarding of Government data. However, they are distinct programs that serve different purposes.

FedRAMP certification applies to specific cloud offerings that create, collect, process, store, or maintain Federal information, while CMMC certification focuses on how organizations protect sensitive government information (FCI and CUI) within their own IT systems.

It is important to note that using FedRAMP-authorized services does not automatically make a company CMMC-compliant. DoD contractors and subcontractors must meet additional security requirements to achieve CMMC compliance.

FedRAMP® vs. CMMC

Key Differences between CMMC and FedRAMP:

Aspect	CMMC	FedRAMP
US Government Agency	Department of Defense (DoD)	All US federal agencies
Who Needs It?	DoD contractor or subcontractor.	Cloud Service Providers (IaaS, PaaS, SaaS) handling federal information.
Purpose	Enforces the protection of sensitive unclassified information for DoD contractors	Promotes and enables secure cloud services adoption across all federal agencies
Scope	DoD contractor IT systems, including cloud and on-premises, handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI)	Cloud services (IaaS, PaaS, SaaS) used or provided by contractors handling federal information
Overlap	Cloud environments used or provided by DoD contractors require FedRAMP Moderate baseline or equivalent compliance to store, process, or transmit CUI entrusted to them.	
Framework	NIST SP 800-171	NIST SP 800-53, FedRAMP baselines
Outcome	Certification for adequate cybersecurity protection in DoD contractor systems	Governmental authorization for cloud services to be used by federal agencies
Compliance Means	CMMC-compliant company can bid on DoD contracts	Authorized Cloud Service Offering can be used for federal projects
Oversight	Department of Defense CIO	Office of Management and Budget (OMB)
Key Documents	DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting	M-24-15 Modernizing the Federal Risk and Authorization Management Program
Resources	DoD CIO CMMC	FedRAMP.gov

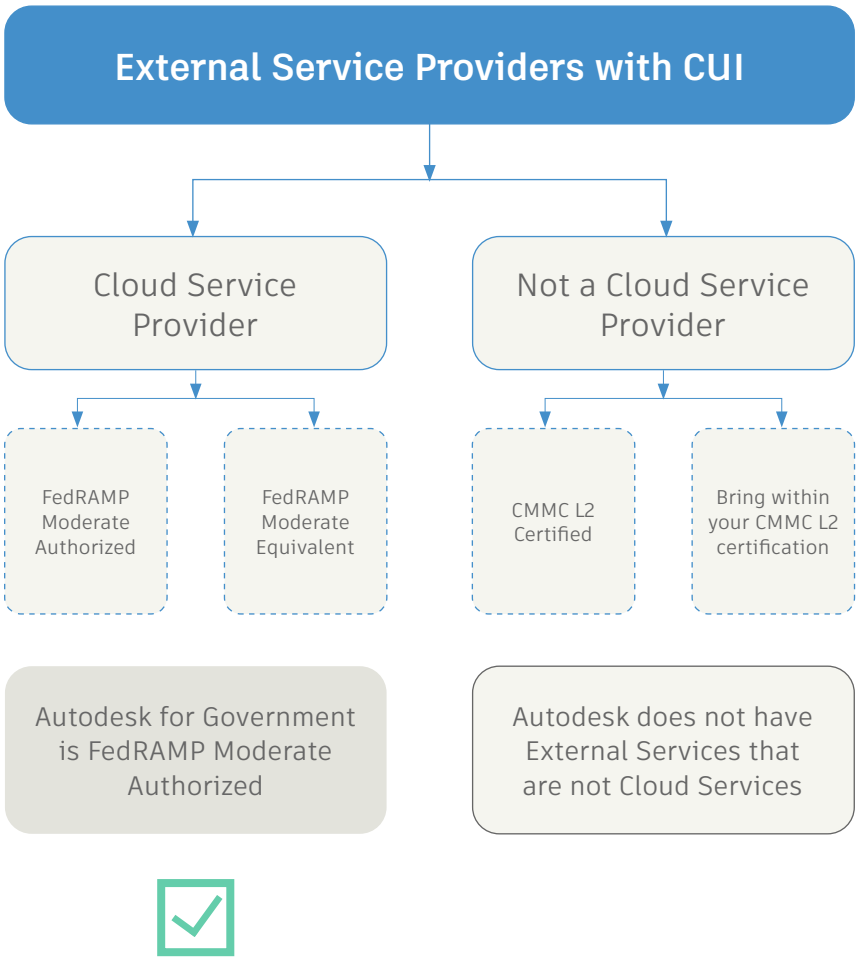
FedRAMP® vs. CMMC

KEY DIFFERENCES BETWEEN CMMC AND FEDRAMP

→ DECISION TREE

The US federal government consists of more than 400 agencies, including the Department of Defense (DoD). FedRAMP was established to help these agencies accelerate cloud service adoption. To meet CMMC Level 2 requirements for Cloud Service Offerings, DoD contractors handling sensitive government information must use FedRAMP Moderate Authorized cloud services (or equivalent).

Autodesk for Government offering is FedRAMP Moderate Authorized and therefore meets these requirements for DoD contractors.



Autodesk for Government

Autodesk for Government is a FedRAMP® Moderate Authorized system compliant with DFARS 252.204–7012 and CMMC Level 2 requirement for Cloud Service Providers (CSP) and Cloud Service Offerings (CSO).

Autodesk for Government connects architecture, engineering, and construction teams in a secure FedRAMP Moderate Authorized cloud environment and provides a single platform to make project collaboration and document management simpler.

Autodesk for Government helps to improve transparency and accountability with a single source of truth for customers collaborating on federal building projects.

Products included in the Autodesk for Government offering:

Autodesk Docs for Government

Provides cloud-based document management and a common data environment in the Autodesk for Government cloud platform. It enables teams to:

- Share information in a FedRAMP® Moderate Authorized cloud environment
- Control project access with approval workflows
- Align team members and simplify project scheduling
- Automate common workflows using Autodesk Platform Services for Government APIs

Autodesk BIM Collaborate Pro for Government

Provides a secure cloud-based design collaboration tool that enables teams to:

- Work together on increasingly complex projects with advanced security requirements.
- Organize project data, manage access, and connect teams.
- Improve project visibility to deliver projects on time.
- Co-author in Revit®

Learn more on Autodesk for Government page.

Explore how Autodesk for Government brings commercial capabilities to federal AEC teams through this whitepaper.

FAQ

1. Is Autodesk CMMC Level 2 compliant?

CMMC Level 2 does not directly apply to Autodesk. However, it may apply to Autodesk customers if they are or plan to become contractors or subcontractors of the US Department of Defense (DoD).

Desktop Products

Autodesk does not have power or control over the security of our customers' IT systems. It is the responsibility of Autodesk users to protect DoD information that is processed, stored, or transmitted on their devices. DoD contractors can use Autodesk desktop products, BUT they must ensure that the security of their IT systems meets CMMC Level 2 requirements.

For example, DoD contractor using AutoCAD® to process CUI on behalf of the DoD must do so only on assets within their CMMC Level 2 assessment scope.

Cloud-Based Products

If DoD vendors will process, store, or transmit CUI shared with them or created by them for DoD in a cloud environment, they need to ensure that Cloud Service Provider (CSP) of their choice is FedRAMP® Moderate Authorized or equivalent. Autodesk for Government offering meets this requirement, which means that DoD contractors and subcontractors can use products included in the Autodesk for Government offering while working with the DoD.

However, Autodesk cloud services that fall outside the Autodesk for Government scope are not FedRAMP Moderate Authorized and do not meet FedRAMP equivalency requirements. Therefore, DoD contractors cannot use these services for handling CUI.

FAQ

2. I need to provide evidence that Autodesk is CMMC compliant. What can I provide?

Autodesk is not a direct subject of CMMC Level 2. However, when Autodesk customers undergo a CMMC Level 2 audit, Autodesk systems may be included as an External Service Provider (ESP) that is a Cloud Service Provider (CSP) that is used to process, store, or transmit Controlled Unclassified Information (CUI).

To be compliant with CMMC, a company needs to assess its entire IT environment and processes to ensure they meet CMMC requirements. A CMMC auditor may want to know the security measures, data handling processes, incident response procedures, etc., implemented by DoD contractor.

Autodesk cannot control or verify the security level of our customers' IT environments. Therefore, Autodesk cannot provide evidence of compliance with CMMC on behalf of our customers. It is the responsibility of Autodesk users to assess their security practices and compliance level according to CMMC requirements.

However, if an Autodesk customer is using products from the Autodesk for Government offering, they can demonstrate that they use a CMMC-compliant Cloud Service Provider by referring to the FedRAMP Marketplace. Autodesk for Government is listed there as FedRAMP® Moderate Authorized: Autodesk for Government | FedRAMP Marketplace.

Important: FedRAMP Moderate authorization applies only to Autodesk for Government offerings. Autodesk cloud products that fall outside the scope of Autodesk for Government are not FedRAMP Authorized and do not meet FedRAMP equivalency requirements.

Example:

Autodesk Docs for Government Cloud Product FedRAMP Moderate-authorized	**CAN BE USED** by the DoD contractor to handle CUI.
Autodesk Docs Cloud Product Not FedRAMP-authorized	**CANNOT BE USED** by the DoD contractor to handle CUI.

FAQ

3. Are any other Autodesk cloud offerings appropriate for my CMMC Level 2 compliance (besides Autodesk for Government)?

If a DoD contractor or subcontractor will process, store, or transmit CUI shared with them or created by them for DoD in a cloud environment, they need to ensure that their chosen Cloud Service Provider (CSP) is FedRAMP Moderate Authorized or FedRAMP equivalent.

To learn more about the requirements for CSPs, see page 6 or refer to the original document for DFARS clause 252.204–7012.

Autodesk for Government is the only offering that is FedRAMP Moderate Authorized.

Achieving FedRAMP "equivalency" is impractical for Autodesk cloud services that are not part of Autodesk for Government. Full compliance is a very difficult threshold for any CSP to meet, and it poses a significant burden on customers. For example, it is the responsibility of the DoD contractor that chooses to use a FedRAMP "equivalent" cloud provider to validate the CSP compliance level themselves and provide the Body of Evidence to the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and assessors.

FAQ

4. Are there limits on the type of CDI or CUI allowed in Autodesk for Government?

There may be limits on the type of Covered Defense Information (CDI) or Controlled Unclassified Information (CUI) allowed in Autodesk for Government. Both CDI and CUI can be subject to more stringent or additional safeguarding or dissemination controls beyond CMMC Level 2 and FedRAMP Moderate requirements. It is important for US Government contract holders to review the relevant regulations and any offerings prior to determining which offering is the best fit to support their CUI obligations.

Resources

CMMC Program Overview from Chief Information Officer, U.S. Department of Defense

CMMC FAQs from Chief Information Officer, U.S. Department of Defense

CMMC Level 2 Scoping Guide

32 CFR Part 170, or "Cybersecurity Maturity Model Certification (CMMC) Program". Final rule established by the U.S. Department of Defense on November 15, 2024.

48 CFR 52.204-21, often referred to as the FAR Clause. Includes 15 basic safeguarding requirements for CMMC Level 1.

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

NIST SP 800-171 Rev. 2. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". Includes 110 security requirements for CMMC Level 2.

NIST SP 800-171 Rev. 3. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

NIST SP 800-172. "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171". Includes 24 security controls required for CMMC Level 3, in addition to those specified in NIST SP 800-171.

U. S. Department of Defense Memorandum from December 2023, often referred to as the "FedRAMP Equivalency Memo"

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

Department of Defense CUI Registry Category List

The following resources provide general information about Autodesk and additional information on topics referenced in this document.

Disclaimer

This document may contain forward-looking statements about our outlook, future results and related assumptions, total addressable markets, acquisitions, products and product capabilities, and strategies. These statements reflect our best judgment based on currently known factors. Actual events or results could differ materially. Please refer to our SEC filings, including our most recent Form 10-K and Form 10-Q filings available at www.sec.gov, for important risks and other factors that may cause our actual results to differ from those in our forward-looking statements.

The forward-looking statements made in this document are being made as of the time and date of its publication, September 2025. If this document is reviewed after the time and date of its publication, even if subsequently made available by us, on our website or otherwise, this document may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statements.

Statements regarding planned or future development efforts for our products and services are not intended to be a promise or guarantee of future availability of products, services, or features, but merely reflect our current plans and are based on factors currently known to us. Purchasing decisions should not be made based upon reliance on these statements.

To learn more about Autodesk, please visit **autodesk.com**

For more information on our comprehensive security framework, please visit **autodesk.com/trust/security**

- Autodesk for Government
- Autodesk Compliance
- Autodesk FedRAMP Authorization Status