

# FileCloud Enables CMMC 2.0 File Sharing and Data Management white paper

FileCloud is a hyper-secure file sharing, remote access, and data governance solution that supports CMMC 2.0 compliance. The single-pane-of-glass experience provides a better path forward for Defense Industrial Base entities to implement and maintain cybersecurity controls.

# Table of Contents

- [How FileCloud Supports CMMC 2.0](#) →
- [Why is CMMC important?](#) →
- [What is CMMC and Who Manages it?](#) →
- [How has CMMC evolved?](#) →
- [CMMC 1.0](#) →
- [CMMC 2.0](#) →
- [Changes Between CMMC 1.0 and 2.0 Levels](#) →
- [CMMC 2.0 Projected Costs](#) →
- [Distinguishing Between Assessment and Certification Costs](#) →
- [FileCloud Supports DIB Entity Compliance with CMMC 2.0](#) →
- [CMMC 2.0 & FileCloud Domain Mapping](#) →
- [CMMC 2.0 & FileCloud Requirements Mapping](#) →
- [Learn More](#) →
- [Glossary of Terms](#) →
- [About FileCloud](#) →



## How FileCloud Supports CMMC 2.0

FileCloud is a hyper-secure file sharing, collaboration, and data governance solution leveraged by major enterprises and organizations around the world, across highly regulated and critical infrastructure industries. Built-in compliance support is available for a variety of regulatory standards, including HIPAA, GDPR, ITAR, NIST 800-171, FIPS 140-2, and CMMC 2.0 (among others).

Powerful governance, security, and access controls within FileCloud provide the requisite infrastructure to support data visibility, organization, and protected access for admins and users alike, all within a streamlined, single-pane-of-glass environment ideal for managing confidential or sensitive information.

By leveraging these functionalities, government contractors and entities can deploy FileCloud as a significant IT infrastructure solution supporting CMMC 2.0 compliance and data management.

In this white paper, we will explore the topic of CMMC in depth, covering the significance of CMMC as a cybersecurity standard developed by the US federal government. We will also briefly review the development of the program from CMMC 1.0 to 2.0, as well as the current implementation plan and the projected costs recently released by the Department of Defense.

Lastly, we will evaluate the specific domains and requirements associated with each CMMC level as they currently stand at the time of this white paper's publication, mapping these requirements to FileCloud's hyper-secure solution.



## Why is CMMC important?

The theft of intellectual property and sensitive information from all industrial sectors due to malicious cyber activity threatens economic and national security. The [World Economic Forum](#) estimates that malicious cyber activity incurred a global cost around \$6 trillion in 2021 – this cost is estimated to grow to \$10 trillion in damages by 2025.

Similarly, the [Center for Strategic and International Studies](#) estimates that the total global cost of cybercrime exceeded \$1 trillion in 2018. Malicious cyber actors have targeted (and continue to target) the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD).

The DIB sectors consist of over 300,000 companies that contribute toward the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services.

The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security.

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working with industries to enhance the protection of the following types of unclassified information within the supply chain.

- **Federal Contract Information (FCI):**

FCI is information provided by or generated for the U.S. government under contract not intended for public release.

- **Controlled Unclassified Information (CUI):**

CUI is a US federal government label, which indicates that marked information requires safeguarding or dissemination controls, consistent with applicable laws, regulations, and other government-wide policies. The CUI program was initially launched in 2010 under [Executive Order 13556](#) to bring greater uniformity for data protection throughout the executive branch.





## What is CMMC and Who Manages it?

The [Office of the Under Secretary of Defense for Acquisition and Sustainment \(OUSD\(A&S\)\)](#) developed the Cybersecurity Maturity Model Certification (CMMC) framework with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB sector.

The original CMMC model measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats. The model has been built out of preexisting cybersecurity standards and best practices across multiple frameworks, and refined according to inputs from the broader community. The current CMMC program is managed by the Department of Defense [Chief Information Officer](#) (DoD CIO).

## How has CMMC Evolved?

The CMMC program is officially a pending program, currently in the rulemaking process, though rollout and testing are well underway. The program has been updated from its initial launch to incorporate public commentary and industry feedback. Once rulemaking is complete, CMMC 2.0 will become a requirement for all DIB contracts.



# CMMC 1.0

## CMMC is based upon two previous US federal mandates:

- Federal Acquisition Regulation (FAR) Clause 52.204-21 – published May 2016 – contractors are mandated to protect systems with the requisite 15 basic cybersecurity requirements to secure FCI.
- Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 – published October 2016 – all government contractors and subcontractors must comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to secure CUI.

CMMC 1.0 was first introduced in September 2020 by the DoD as an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041). This interim rule established the three basic features of the CMMC framework:

- Tiered model – CMMC offers different levels of compliance that consider the information being handled and security needs.
- Required assessments – Certification of compliance by either third-party assessors or government partners
- Implementation through contracts – contracts issued by the federal government will require CMMC compliance.

The CMMC model adds a certification element to the previous mandates. Certifications serves to verify that cybersecurity processes and practices toward a specific maturity level have been implemented. CMMC certification specifically provides increased assurance to the DoD that a DIB contractor adequately protects CUI throughout the flow of information between company employees, subcontractors, and suppliers.

Three additional regulations were added in [November 2020](#).

- **DFARS 252.204-7019** - Requires contractors and subcontractors to upload their summary level score for their NIST SP 800-171 DoD assessment (Basic, Medium, or High) to the DoD Supplier Performance Risk System (SPRS).
- **DFARS 252.204-7020** – Establishes the right of the government to audit companies; audits will be carried out by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Companies must provide the government with access to their systems and facilities and verify that subcontractors are compliant.
- **DFARS 252.204-7021** – As of October 1, 2025, CMMC will be required by contract award. Prior to this rollout date, the Office of the Undersecretary of Defense for Acquisition & Sustainment [OUSD(A&S)] must approve the inclusion of CMMC in new acquisitions. The level of mandated CMMC certification must be maintained throughout the contract award period.



# CMMC 1.0 Levels

The CMMC program organizes cybersecurity requirements across several levels. To even bid on a contract, DIB contractors must be able to prove, via certification, that they can meet the CMMC level requirements set by the DoD.

CMMC 1.0 included 5 levels total, with levels 2 and 4 serving as transitional levels to 3 and 5, respectively.

DIB contractors can be assessed and certified across their entire organization or for particular divisions and departments, depending on where protected information is stored and how it is processed.

## Level 1 – Basic Cyber Hygiene

Includes basic cybersecurity suitable for small companies having a subset of universally accepted common practices. The processes at this level would include some basic performed cybersecurity practices. This level has 35 security controls that must be implemented successfully.

## Level 2 – Intermediate Cyber Hygiene

Includes universally accepted cybersecurity best practices. Practices at this level should be documented, and access to CUI will require multi-factor authentication. This level includes an additional 115 security controls on top of Level 1.

## Level 3 – Good Cyber Hygiene

Includes coverage of all NIST SP 800-171 Rev. 1 controls and additional practices beyond the scope of current CUI protection. Processes at this level are maintained, and there is a comprehensive knowledge of cyber assets. This level requires an additional 91 security controls on top of those covered in Levels 1 and 2.

## Level 4 – Proactive

Includes advanced and sophisticated cybersecurity practices. The processes at this level are periodically reviewed, properly resourced, and are improved regularly across the enterprise. In addition, the defensive responses operate at high speed and there is a knowledge of all cyber assets. This level has an additional 95 controls on top of the first three levels.

## Level 5 – Advanced / Progressive

Includes highly advanced cybersecurity practices. The processes involved at this level include continuous improvement across the enterprise and defensive responses performed at high speed. This level requires an additional 34 controls.



# CMMC 2.0

The interim rule establishing CMMC 1.0 became effective on November 30, 2020, with more than 850 public comments filed in response. These comments highlighted confusion and trepidation around implementation of CMMC, prompting an internal review. This review was carried out in March 2021 by cybersecurity and acquisition leaders within DoD to refine the compliance policy and implementation processes.

Following the internal review, the DoD published an [Advance Notice of Proposed Rulemaking \(ANPRM\)](#) on November 17, 2021. The proposed changes comprise CMMC 2.0 and will take effect after the rulemaking process is completed.

Rulemaking will be completed within Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Per the CMMC information page on the DoD CIO website, CMMC 2.0 is still technically within the rulemaking process; however, CMMC 2.0 has passed through the initial public comment period, as well as the Office of Management and Budget review. On December 26, 2024, the DoD submitted [Rule Proposal 88 FR 89058](#), with the public commentary period closing on February 26, 2024.

In the meantime, all CMMC pilot programs have been suspended, and certification is not required for any contract until rules have been finalized, including a 60-day public comment period prior to the rule taking effect.

However, the DoD is continuing to urge DIB contractors to evaluate their cybersecurity protocols, organize documentation, and generally prepare for CMMC implementation and enforcement. The DoD's current timeline projects that CMMC 2.0 requirements will be in place for all contract solicitations on or after October 1, 2026 (though waivers may be issued depending on CMMC program developments and the specific contract details). The DoD has also launched [Project Spectrum](#) to support DIB companies in assessing cyber readiness and adopting cybersecurity best practices.

**DoD currently requires covered defense contractors and subcontractors to implement the security protections** set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800-171 Rev 2 requirement not yet implemented, in a System Security Plan (SSP).





## Key Changes from CMMC 1.0 to 2.0

**More Speed and Flexibility** – Allows waivers of CMMC requirements and lets companies create Plans of Action & Milestones to obtain certification under certain circumstances.

**Less Expensive** – Allows all Level 1 (Foundational) and a subset at Level 2 (Advanced) to show compliance through self-assessments.

**Streamlined Requirements** – CMMC 2.0 focuses on the most critical requirements, reducing the model from 5 to 3 compliance levels.

**Use of Widely Accepted Standards** – The model now uses National Institute of Standards and Technology's (NIST) cybersecurity standards and removes CMMC-unique practices.

**More Accountability** – Increases oversight of professional and ethical standards of third-party assessors.

**Reduction of Tiers** - One of the most obvious changes from CMMC 1.0 to 2.0 is the reduction of tiers from 5 levels to 3. This change removes “transitional” certification levels and clarifies the certification requirements for each level.

## CMMC 2.0 Certification Levels

### Level 1 – Foundational:

Matches 15 controls from FAR 52.204-21 “basic” controls to protect FCI. Annual certifications and self-assessments are completed by company leadership. Equivalent to previous Level 1.

### Level 2 – Advanced:

Based upon the old CMMC 1.0 Level 3; lowers the number of required controls to 110 controls in the SP 800-171 Revision. 2 (NIST SP 800171). This eliminates 20 additional CMMC 1.0 Level 3 controls.

CMMC will distinguish between “prioritized” and “nonprioritized” acquisitions based on the sensitivity of CUI. Prioritized acquisitions may handle CUI related to defense systems, whereas nonprioritized acquisitions may include information on military uniforms. Future rulemakings will likely provide greater detail on prioritization.

Prioritized acquisitions will need to be reviewed by a Certified Third-Party Assessor Organization (C3PAO) every three years. Nonprioritized acquisitions will be subject to less scrutiny, requiring only an annual self-assessment and certification.

### Level 3 – Expert:

Replaces Levels 4 and 5 in CMMC 1.0. Acquisitions at the new Level 3 “Expert” level require triennial, government-led assessments. This level also requires compliance with the 110 controls stipulated in the new Level 2 certification as well as NIST's SP 800-172. This level of certification will not be required by most DIB contractors.



## Changes between CMMC 1.0 and 2.0 Levels.

| CMMC Model 1.0          |                                   |             |   |
|-------------------------|-----------------------------------|-------------|---|
| Model                   | Assessment                        | Level       |   |
| <b>171</b><br>Practices | <b>5</b><br>Processes             | Third-party | <b>LEVEL 5</b><br>Advanced<br><i>CUI, Critical Programs</i> |
| <b>156</b><br>Practices | <b>4</b><br>Processes             | None        | <b>LEVEL 4</b><br>Proactive<br><i>Transition Level</i>      |
| <b>130</b><br>Practices | <b>3</b><br>Processes             | Third-party | <b>LEVEL 3</b><br>Good<br><i>CUI</i>                        |
| <b>72</b><br>Practices  | <b>2</b><br>Maturity<br>Processes | None        | <b>LEVEL 2</b><br>Intermediate<br><i>Transition Level</i>   |
| <b>17</b><br>Practices  |                                   | Third-party | <b>LEVEL 1</b><br>Basic<br><i>FCI Only</i>                  |

| CMMC Model 2.0 |   |  |
|----------------|---|--|
| Level          | Model   | Assessment   |
| <b>LEVEL 3</b> | <b>134</b><br>Requirements based<br>on NIST SP 800-171<br>and 800-172 | Triennial government-led<br>assessment & annual<br>affirmation   |
| <b>LEVEL 2</b> | <b>110</b><br>Requirements aligned<br>with NIST SP 800-171<br>Rev 2   | Triennial third-party<br>assessment & annual<br>affirmation: Triennial self-<br>assessment & annual<br>affirmation for select programs |
| <b>LEVEL 1</b> | <b>15</b><br>Requirements<br>aligned with FAR<br>52.204-21            | Annual self-assessment   |





## CMMC 2.0 Projected Costs

There is no easy answer to how much CMMC 2.0 will cost DIB contractors. The total cost will vary depending on the sensitivity of data handled, the number of users in a system, the existing cybersecurity infrastructure, and the CMMC Level required by the specific contract.

Current contracts may not include CMMC as a requirement, and CMMC cannot be applied retroactively to contracts. However, once CMMC 2.0 is rolled out, compliance will be a prerequisite for all new DOD contracts. Without the requisite certification, contractors will not be able to bid on future contracts.

The DoD's Proposed Rule, published December 26, 2023, reviews the potential costs affiliated with CMMC 2.0 implementation according to the relevant requirements level. Full breakdowns of projected costs can be found within the [Proposed Rule](#).



**Summary of Estimated Public Costs to Implement CMMC 2.0 —  
All DIB Contractors & Subcontractors not defined as a "Small Entity"**

| Assessment Phase (\$)           | Level 1 Self-Assesment | Level 2 Self-Assesment | Level 2 Certification | Level 3 Certification |
|---------------------------------|------------------------|------------------------|-----------------------|-----------------------|
| Periodicity                     | Annual                 | Triennial              | Triennial             | Triennial             |
| Plan and Prepare the Assessment | \$1,146                | \$18,015               | \$26,264              | \$7,066               |
| Conduct the Assessment          | \$1,728                | \$19,964               | \$80,656              | \$23,136              |
| Report Assessment Results       | \$584                  | \$2,712                | \$2,712               | \$2,712               |
| Annual Affirmation(s)           | \$584                  | *\$8,136               | *\$8,136              | *\$8,136              |
| Subtotal                        | \$4,042                | \$48,827               | \$117,768             | \$41,050              |
| ** POA&M                        | \$0                    | \$0                    | \$0                   | \$3,394               |
| <b>Total (Across 3 Years)</b>   | <b>\$4,042</b>         | <b>\$48,827</b>        | <b>\$117,768</b>      | <b>\$44,444</b>       |

\*Reflects the 3-year cost to match the periodicity | \*\*Requirements NOT MET (if needed and when allowed) will be documented in a Plan of Action and Milestones

Table 7, [Proposed Rule 89 FR 13013](#)





**Summary of Estimated Public Costs to Implement CMMC 2.0 —  
All DIB Contractors, Subcontractors, and other entities defined as a "Small Entity"**

| Assessment Phase (\$)           | Level 1 Self-Assesment | Level 2 Self-Assesment | Level 2 Certification Assessment | Level 3 Certification Assessment |
|---------------------------------|------------------------|------------------------|----------------------------------|----------------------------------|
| Periodicity                     | Annual                 | Triennial              | Triennial                        | Triennial                        |
| Plan and Prepare the Assessment | \$1,803                | \$14,426               | \$20,699                         | \$1,905                          |
| Conduct the Assessment          | \$2,705                | \$15,542               | \$76,743                         | \$1,524                          |
| Report Assessment Results       | \$909                  | \$2,851                | \$2,851                          | \$1,876                          |
| Affirmations                    | \$560                  | *\$4,377               | *\$4,377                         | *\$5,628                         |
| Subtotal                        | \$5,977                | \$37,196               | \$104,670                        | \$10,933                         |
| **POA&M                         | \$0                    | \$0                    | \$0                              | \$1,869                          |
| <b>Total</b>                    | <b>\$5,977</b>         | <b>\$37,196</b>        | <b>\$104,670</b>                 | <b>\$12,802</b>                  |

\*Reflects the 3-year cost to match the periodicity | \*\*Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones

Table 8, [Proposed Rule 89 FR 13013](#)



The full breakdown of projected costs is organized across the different CMMC levels, the assessment time frames (annual or triennial), and the different types of expenses, which include:

#### **Nonrecurring Engineering Costs:**



Hardware, software, and the associated labor to implement.

#### **Recurring engineering costs:**



Annually recurring fees and associated labor for technology refresh.

#### **Assessment Costs:**



Activities for pre-assessment preparations (which includes gathering and/or developing evidence that the assessment objectives for each requirement have been satisfied), conducting and/or participating in the actual assessment, and completion of any post-assessment work.

#### **Affirmation Costs for Each CMMC Level:**



Costs for an OSA to submit to SPRS an initial and, as applicable, any subsequent affirmations of compliance that the contractor information system is compliant with and will maintain compliance with the security requirements of the applicable CMMC Level.

However, these projected cost tables do not include the costs of implementing nonrecurring and recurring engineering expenses for CMMC levels 1 and 2; these requirements are already captured by FAR clause 52.204–21, which went into effect June 15, 2016, and by DFARS clause 252.204–7012, which went into effect December 31, 2017, respectively.

As a result, these expenses should already have been budgeted for and incurred by contractors and entities currently working on federal contracts or currently bidding on proposed contracts.





## Distinguishing Between Assessment and Certification Costs

Assessment costs are another layer of expense for any contractors seeking level 2 or 3 certification. This is the difference between compliance costs (cybersecurity investment) and certification costs. CMMC Levels 2 and 3 each require annual affirmations. Level 3 certification must be carried out every three years by government-led assessors. Level 2 certification must be carried out every three years by C3PAOs.

A subset of Level 2 designated contracts (contracts that include non-prioritized CUI), as well as Level 1 contracts, will be able to self-assess, meaning they will not be subject to certification costs.

The DoD CIO anticipates that most contractors will need Level 2 certification. To ensure successful certification by 3PCAO or federal auditors, DIB contractors may also opt to conduct preliminary gap assessments prior to their certification audit.

### Infrastructure Investment and Remediation Costs

Companies with mature solutions for NIST 800-171 compliance will find that their overall CMMC compliance costs will be much lower. They have already invested in security hardening and access controls that answer many CMMC requirements.

Costs will be much higher for companies that need to implement brand new solutions. There will also be costs associated with infrastructure maintenance (recurring annual costs). These costs can be in the tens or even hundreds of thousands of dollars if it involves migrating from a public consumer product to a specialized compliant environment. Costs may be mitigated by opting instead for a self-hosted solution like FileCloud that provides guidance on compliant configurations and settings.



## FileCloud Supports DIB Entity Compliance with CMMC 2.0

The DoD will include a specific CMMC level as a requirement for all contracts once the program is fully implemented; select contracts will be identified as part of the programs phased rollout, meaning that some DIB contractors and entities will undergo CMMC ahead of others.

DIB entities can use FileCloud Server, FileCloud's self-hosted solution, to meet many of these CMMC requirements, easing the resource burdens (time, expertise, financial, etc.) associated with the program's assessment and certification processes.

### Map FileCloud to CMMC 2.0 Domains

CMMC requirements are organized into specific security domains. CMMC 1.0 included 17 domains, but with the release of CMMC 2.0, the number of domains has been cut back to 14. Specifically, the Asset Management, Recovery, and Situational Awareness domains have been removed; Risk Management has been changed to Risk Assessment.

As part of this white paper, we have included a table that maps FileCloud Server's powerful functionalities to CMMC 2.0 domains across Levels 1, 2, and 3.





## Cybersecurity Maturity Model Certification (CMMC) 2.0

| Domain                      | Requirements   | How Does FileCloud Server Comply?  |
|-----------------------------|--|--|
| Access Control (AC)         | <ul style="list-style-type: none"><li>• Establish system access requirements</li><li>• Control internal system access</li><li>• Control remote system access</li><li>• Limit data access to authorized users and processes</li></ul> | <ul style="list-style-type: none"><li>• Admin-controlled user profiles and user groups</li><li>• Granular file/folder permissions for users or groups</li><li>• Integrations: Active Directories (AD), LDAP, SSO, Network Shares, and NTFS permissions</li><li>• Data Leak Prevention (DLP) allows or denies file shares/downloads</li><li>• Role Based Access Control (RBAC) for admin users</li><li>• Access policies for connected remote devices</li></ul> |
| Awareness and Training (AT) | <ul style="list-style-type: none"><li>• Conduct security awareness activities</li><li>• Conduct training</li></ul>   | <p>FileCloud provides complementary support to help optimize your FileCloud environment:</p> <ul style="list-style-type: none"><li>• FileCloud resource library on best security practices</li><li>• FileCloud University (training videos)</li><li>• Customer Support</li><li>• Professional Services</li></ul>   |



| Domain                          | Requirements   | How Does FileCloud Server Comply?   |
|---------------------------------|--|---|
| <b>Audit and Accountability</b> | <ul style="list-style-type: none"> <li>• Define audit requirements</li> <li>• Perform auditing</li> <li>• Identify and protect audit information</li> <li>• Review and manage audit logs</li> </ul>  | <ul style="list-style-type: none"> <li>• Comprehensive audit logs (capture who accessed what data, with time stamps, IP addresses, and connected device information – who, what, when, where, &amp; how)</li> <li>• Audit log is unchangeable and can be exported for ease of review</li> <li>• SIEM integration</li> <li>• Hierarchical retention policies</li> <li>• Access/modification restrictions on specified records</li> </ul> |
| <b>Incident Response (IR)</b>   | <ul style="list-style-type: none"> <li>• Plan incident response</li> <li>• Detect and report events</li> <li>• Develop and implement response to a declared incident</li> <li>• Perform post incident reviews</li> <li>• Test incident response</li> </ul> | <ul style="list-style-type: none"> <li>• Data governance dashboard displays potential rule violations (e.g., DLP, retention policies).</li> <li>• SIEM integration</li> <li>• Admin &amp; user-based workflow automation: workflows support automated report generation, device approval, and other tasks.</li> </ul>   |
| <b>Media Protection</b>         | <ul style="list-style-type: none"> <li>• Identify and mark media</li> <li>• Protect and control media</li> <li>• Sanitize media</li> <li>• Protect media during transport</li> </ul>   | <ul style="list-style-type: none"> <li>• Integrated antivirus via ClamAV or ICAP protocol scans uploaded files</li> <li>• DLP provides granular control over data</li> <li>• In-transit encryption via HTTPS (SSL/TLS) protocols</li> </ul>   |



| Domain                                 | Requirements   | How Does FileCloud Server Comply?   |
|--|--|---|
| Configuration Management (CM)          | <ul style="list-style-type: none"> <li>Establish configuration baselines</li> </ul>      | <p>FileCloud contains multiple configuration capabilities, including but not limited to:</p> <ul style="list-style-type: none"> <li>Centralized device management</li> <li>Content classification</li> <li>DLP</li> <li>Global policies</li> <li>Device configuration policies</li> <li>Customization</li> <li>Data governance</li> <li>User password enforcement</li> <li>Private sharing permissions</li> <li>Granular folder-level permissions</li> <li>Configuration guides and examples (Support Documentation)</li> </ul> |
| Identification and Authentication (IA) | <ul style="list-style-type: none"> <li>Grant access to authenticated entities</li> </ul> | <ul style="list-style-type: none"> <li>Proprietary user authentication</li> <li>AD/LDAP integration</li> <li>Network shares integration</li> <li>SSO &amp; 2FA</li> </ul>   |



| Domain                   | Requirements  | How Does FileCloud Server Comply?  |
|--------------------------|---|--|
| Maintenance (MA)         | <ul style="list-style-type: none"> <li>Manage maintenance</li> </ul>  | <ul style="list-style-type: none"> <li>Workflows automate maintenance tasks within FileCloud; e.g.,               <ul style="list-style-type: none"> <li>Deleting files after a specified amount of time</li> <li>Disabling users who have not accessed FileCloud after a set number of days</li> </ul> </li> <li>Automatic audit log trimming and export to a location defined by the administrator</li> <li>Automatic backup capabilities (backupserver system)</li> <li>Internal system scheduled tasks (CRON)</li> </ul> |
| Personnel Security (PS)  | <ul style="list-style-type: none"> <li>Screen personnel</li> <li>Protect CUI during personnel actions</li> </ul>                    | <ul style="list-style-type: none"> <li>Smart Classification + DLP automates classification and application of DLP rules that deny or permit downloading/sharing.</li> </ul>  |
| Physical Protection (PE) | <ul style="list-style-type: none"> <li>Limit physical access</li> </ul>   | Not Applicable   |
| Risk Assessment (RA)     | <ul style="list-style-type: none"> <li>Identify and evaluate risk</li> <li>Manage risk</li> <li>Manage supply chain risk</li> </ul> | Not Applicable   |





| Domain                                     | Requirements  | How Does FileCloud Server Comply?   |
|--|---|---|
| Security Assessment (CA)                   | <ul style="list-style-type: none"> <li>• Develop and manage a system security plan</li> <li>• Define and manage controls</li> <li>• Perform code reviews</li> </ul>   | Not Applicable  |
| Systems and Communications Protection (SC) | <ul style="list-style-type: none"> <li>• Define security requirements for systems and communications</li> <li>• Control communications at system boundaries</li> </ul>  | <ul style="list-style-type: none"> <li>• Separate login portals for admins and users</li> <li>• Granular access permissions for users or groups</li> <li>• DLP rules that permit or deny downloading/sharing of data</li> <li>• Encryption for data at rest and in transit</li> <li>• Configure FileCloud in FIPS mode (encryption + additional security features)</li> <li>• Client/customer key management support</li> </ul> |
| System and Information Integrity (SI)      | <ul style="list-style-type: none"> <li>• Identify and manage information system flaws</li> <li>• Identify malicious content</li> <li>• Perform network and system monitoring</li> <li>• Implement advanced email protections</li> </ul> | Not Applicable  |





## Map FileCloud to CMMC 2.0 Requirements

CMMC domains can be further broken down into explicit requirements, according to each CMMC certification level. These requirements have been mapped in a spreadsheet according to domain and certification level. This requirements spreadsheet can be downloaded directly from the DoD CIO's CMMC web page, under [Documentation](#).

FileCloud has created a custom checklist based on the CMMC spreadsheet resource. This checklist notates which CMMC requirements can be met by FileCloud features and functionalities, compared to those which must be met outside of the software environment, in line with the shared responsibility model for cloud providers and customers.



# Access Control (AC)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 1      |  |           |
| AC.L1-3.1.1  | <b>Authorized Access Control</b><br>Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | ✓         |
| AC.L1-3.1.2  | <b>Transaction &amp; Function Control</b><br>Limit information system access to the types of transactions and functions that authorized users are permitted to execute.                    | ✓         |
| AC.L1-3.1.20 | <b>External Connections</b><br>Verify and control/limit connections to and use of external information systems.  | ✓         |
| AC.L1-3.1.22 | <b>Control Public Information</b><br>Control information posted or processed on publicly accessible information systems.   | ✓         |
| Level 2      |  |           |
| AC.L2-3.1.3  | <b>Control CUI Flow</b><br>Control the flow of CUI in accordance with approved authorizations.   | ✓         |



## Access Control (AC)

| CMMC 2.0    | Details  | FileCloud |
|-------------|--|-----------|
| Level 2     |  |           |
| AC.L2-3.1.4 | <b>Separation of Duties</b><br>Separate the duties of individuals to reduce the risk of malevolent activity without collusion.                             | ✓         |
| AC.L2-3.1.5 | <b>Least Privilege</b><br>Employ the principle of least privilege, including for specific security functions and privileged accounts.                      | ✓         |
| AC.L2-3.1.6 | <b>Non-Privileged Account Use</b><br>Use non-privileged accounts or roles when accessing nonsecurity functions.  | ✓         |
| AC.L2-3.1.7 | <b>Privileged Functions</b><br>Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | ✓         |
| AC.L2-3.1.8 | <b>Unsuccessful Logon Attempts</b><br>Limit unsuccessful logon attempts.   | ✓         |
| AC.L2-3.1.9 | <b>Privacy &amp; Security Notices</b><br>Provide privacy and security notices consistent with applicable CUI rules.  | ✓         |



# Access Control (AC)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 2      |  |           |
| AC.L2-3.1.10 | <b>Session Lock</b><br>Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. | ✓         |
| AC.L2-3.1.11 | <b>Session Termination</b><br>Terminate (automatically) a user session after a defined condition.  | ✓         |
| AC.L2-3.1.12 | <b>Control Remote Access</b><br>Monitor and control remote access sessions.  | ✓         |
| AC.L2-3.1.13 | <b>Remote Access Confidentiality</b><br>Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.        | ✓         |
| AC.L2-3.1.14 | <b>Remote Access Routing</b><br>Route remote access via managed access control points.   | ✓         |
| AC.L2-3.1.15 | <b>Privileged Remote Access</b><br>Authorize remote execution of privileged commands and remote access to security-relevant information. | ✓         |



Access Control (AC)

| CMMC 2.0     | Details   | FileCloud |
|--------------|---|-----------|
| Level 2      |   |           |
| AC.L2-3.1.16 | <b>Wireless Access Authorization</b><br>Authorize wireless access prior to allowing such connections. | N/A       |
| AC.L2-3.1.17 | <b>Wireless Access Protection</b><br>Protect wireless access using authentication and encryption.     | N/A       |
| AC.L2-3.1.18 | <b>Mobile Device Connection</b><br>Control connection of mobile devices.                              | ✓         |
| AC.L2-3.1.19 | <b>Encrypt CUI on Mobile</b><br>Encrypt CUI on mobile devices and mobile computing platforms.         | ✓         |
| AC.L2-3.1.21 | <b>Portable Storage Use</b><br>Limit use of portable storage devices on external systems.             | N/A       |



## Awareness and Training (AT)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| AT.L2-3.2.1 | <b>Role-Based Risk Awareness</b><br>Ensure that managers, systems 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. | N/A       |
| AT.L2-3.2.2 | <b>Role-Based Training</b><br>Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.   | N/A       |
| AT.L2-3.2.3 | <b>Insider Threat Awareness</b><br>Provide security awareness training on recognizing and reporting potential indicators of insider threat.   | N/A       |





# Audit and Accountability (AU)

| CMMC 2.0    | Details  | FileCloud |
|-------------|--|-----------|
| Level 2     |  |           |
| AU.L2-3.3.1 | <b>System Auditing</b><br>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.L2-3.3.2 | <b>User Accountability</b><br>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.L2-3.3.3 | <b>Event Review</b><br>Review and update logged events.  | ✓         |
| AU.L2-3.3.4 | <b>Audit Failure Alerting</b><br>Alert in the event of an audit logging process failure.   | ✓         |
| AU.L2-3.3.5 | <b>Audit Correlation</b><br>Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.       | ✓         |



## Audit and Accountability (AU)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| AU.L2-3.3.6 | <b>Reduction &amp; Reporting</b><br>Provide audit record reduction and report generation to support on-demand analysis and reporting.   | ✓         |
| AU.L2-3.3.7 | <b>Authoritative Time Source</b><br>Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | ✓         |
| AU.L2-3.3.8 | <b>Audit Protection</b><br>Protect audit information and audit logging tools from unauthorized access, modification, and deletion.  | ✓         |
| AU.L2-3.3.9 | <b>Audit Management</b><br>Limit management of audit logging functionality to a subset of privileged users.   | ✓         |



# Configuration Management (CM)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| CM.L2-3.4.1 | <b>System Baselineing</b><br>Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | N/A       |
| CM.L2-3.4.2 | <b>Security Configuration Enforcement</b><br>Establish and enforce security configuration settings for information technology products employed in organizational systems.  | N/A       |
| CM.L2-3.4.3 | <b>System Change Management</b><br>Track, review, approve or disapprove, and log changes to organizational systems.   | N/A       |
| CM.L2-3.4.4 | <b>Security Impact Analysis</b><br>Analyze the security impact of changes prior to implementation.  | N/A       |
| CM.L2-3.4.5 | <b>Access Restrictions for Change</b><br>Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.   | N/A       |



# Configuration Management (CM)

| CMMC 2.0    | Details  | FileCloud |
|-------------|--|-----------|
| Level 2     |  |           |
| CM.L2-3.4.6 | <b>Least Functionality</b><br>Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.  | N/A       |
| CM.L2-3.4.7 | <b>Nonessential Functionality</b><br>Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.  | N/A       |
| CM.L2-3.4.8 | <b>Application Execution Policy</b><br>Apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software. | N/A       |
| CM.L2-3.4.9 | <b>User-Installed Software</b><br>Control and monitor user-installed software.   | N/A       |



# Identification and Authentication (IA)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 1     |   |           |
| IA.L1-3.5.1 | <b>Identification</b><br>Identify information system users, processes acting on behalf of users, or devices.  | ✓         |
| IA.L1-3.5.2 | <b>Authentication</b><br>Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | ✓         |
| Level 2     |   |           |
| IA.L2-3.5.3 | <b>Multifactor Authentication</b><br>Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.          | ✓         |



## Identification and Authentication (IA)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| IA.L2-3.5.4 | <b>Replay-Resistant Authentication</b><br>Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | ✓         |
| IA.L2-3.5.5 | <b>Identifier Reuse</b><br>Prevent reuse of identifiers for a defined period.   | ✓         |
| IA.L2-3.5.6 | <b>Identifier Handling</b><br>Disable identifiers after a defined period of inactivity.   | ✓         |
| IA.L2-3.5.7 | <b>Password Complexity</b><br>Enforce a minimum password complexity and change of characters when new passwords are created.                              | ✓         |
| IA.L2-3.5.8 | <b>Password Reuse</b><br>Prohibit password reuse for a specified number of generations.   | ✓         |
| IA.L2-3.5.9 | <b>Temporary Passwords</b><br>Allow temporary password use for system logons with an immediate change to a permanent password.                            | ✓         |





## Identification and Authentication (IA)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 2      |  |           |
| IA.L2-3.5.10 | <b>Cryptographically-Protected Passwords</b><br>Store and transmit only cryptographically-protected passwords. | ✓         |
| IA.L2-3.5.11 | <b>Obscure Feedback</b><br>Obscure feedback of authentication information.                                     | ✓         |

## Incident Response (IR)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| IR.L2-3.6.1 | <b>Incident Handling</b><br>Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | N/A       |
| IR.L2-3.6.2 | <b>Incident Reporting</b><br>Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.   | N/A       |



# Incident Response (IR)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| IR.L2-3.6.3 | <b>Incident Response Testing</b><br>Test the organizational incident response capability. | N/A       |

# Maintenance (MA)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| MA.L2-3.7.1 | <b>Perform Maintenance</b><br>Perform maintenance on organizational systems.  | N/A       |
| MA.L2-3.7.2 | <b>System Maintenance Control</b><br>Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. | N/A       |



Maintenance (MA)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 2     |   |           |
| MA.L2-3.7.3 | <b>Equipment Sanitization</b><br>Ensure equipment removed for off-site maintenance is sanitized of any CUI.   | N/A       |
| MA.L2-3.7.4 | <b>Media Inspection</b><br>Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  | N/A       |
| MA.L2-3.7.5 | <b>Nonlocal Maintenance</b><br>Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | N/A       |
| MA.L2-3.7.6 | <b>Maintenance Personnel</b><br>Supervise the maintenance activities of maintenance personnel without required access authorization.  | N/A       |



# Media Protection (MP)

| CMMC 2.0    | Details   | FileCloud |
|-------------|---|-----------|
| Level 1     |   |           |
| MP.L1-3.8.3 | <b>Perform Maintenance</b><br>Perform maintenance on organizational systems.  | N/A       |
| Level 2     |   |           |
| MP.L2-3.8.1 | <b>Media Protection</b><br>Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | N/A       |
| MP.L2-3.8.2 | <b>Media Access</b><br>Limit access to CUI on system media to authorized users.   | ✓         |
| MP.L2-3.8.4 | <b>Media Markings</b><br>Mark media with necessary CUI markings and distribution limitations.   | ✓         |



# Media Protection (MP)

| CMMC 2.0    | Details  | FileCloud |
|-------------|--|-----------|
| Level 2     |  |           |
| MP.L2-3.8.5 | <b>Media Accountability</b><br>Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.  | N/A       |
| MP.L2-3.8.6 | <b>Portable Storage Encryption</b><br>Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | N/A       |
| MP.L2-3.8.7 | <b>Removable Media</b><br>Control the use of removable media on system components.   | N/A       |
| MP.L2-3.8.8 | <b>Shared Media</b><br>Prohibit the use of portable storage devices when such devices have no identifiable owner.  | N/A       |
| MP.L2-3.8.9 | <b>Protect Backups</b><br>Protect the confidentiality of backup CUI at storage locations.  | N/A       |



## Personnel Security (PS)

| CMMC 2.0    | Details  | FileCloud |
|-------------|--|-----------|
| Level 2     |  |           |
| PS.L2-3.9.1 | <b>Screen Individuals</b><br>Screen individuals prior to authorizing access to organizational systems containing CUI.  | N/A       |
| PS.L2-3.9.2 | <b>Personnel Actions</b><br>Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | N/A       |

## Physical Protection (PE)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 1      |  |           |
| PE.L1-3.10.1 | <b>Limit Physical Access</b><br>Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | N/A       |





# Physical Protection (PE)

| CMMC 2.0     | Details   | FileCloud |
|--------------|---|-----------|
| Level 1      |   |           |
| PE.L1-3.10.3 | <b>Escort Visitors</b><br>Escort visitors and monitor visitor activity.   | N/A       |
| PE.L1-3.10.4 | <b>Physical Access Logs</b><br>Maintain audit logs of physical access.  | N/A       |
| PE.L1-3.10.5 | <b>Manage Physical Access</b><br>Control and manage physical access devices.  | N/A       |
| Level 2      |   |           |
| PE.L2-3.10.2 | <b>Monitor Facility</b><br>Protect and monitor the physical facility and support infrastructure for organizational systems. | N/A       |
| PE.L2-3.10.6 | <b>Alternative Work Sites</b><br>Enforce safeguarding measures for CUI at alternate work sites.                             | N/A       |



Risk Assessment (RA)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 2      |  |           |
| RA.L2-3.11.1 | <p><b>Risk Assessments</b></p> <p>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.</p> | N/A       |
| RA.L2-3.11.2 | <p><b>Vulnerability Scan</b></p> <p>Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.</p>   | N/A       |
| RA.L2-3.11.3 | <p><b>Vulnerability Remediation</b></p> <p>Remediate vulnerabilities in accordance with risk assessments.</p>  | N/A       |



# Security Assessment (CA)

| CMMC 2.0     | Details   | FileCloud |
|--------------|---|-----------|
| Level 2      |   |           |
| CA.L2-3.12.1 | <b>Security Control Assessments</b><br>Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.   | N/A       |
| CA.L2-3.12.2 | <b>Plan of Action</b><br>Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  | N/A       |
| CA.L2-3.12.3 | <b>Security Control Monitoring</b><br>Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  | N/A       |
| CA.L2-3.12.4 | <b>System Security Plan</b><br>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. | N/A       |



# System and Communications Protection (SC)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 1      |  |           |
| SC.L1-3.13.1 | <b>Boundary Protection</b><br>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. | N/A       |
| SC.L1-3.13.5 | <b>Public-Access System Separation</b><br>Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | N/A       |
| Level 2      |  |           |
| SC.L2-3.13.2 | <b>Security Engineering</b><br>Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  | N/A       |
| SC.L2-3.13.3 | <b>Role Separation</b><br>Separate user functionality from system management functionality.  | ✓         |



## System and Communications Protection (SC)

| CMMC 2.0     | Details   | FileCloud |
|--------------|---|-----------|
| Level 2      |   |           |
| SC.L2-3.13.4 | <b>Shared Resource Control</b><br>Prevent unauthorized and unintended information transfer via shared system resources.   | ✓         |
| SC.L2-3.13.6 | <b>Network Communication by Exception</b><br>Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).  | ✓         |
| SC.L2-3.13.7 | <b>Split Tunneling</b><br>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). | N/A       |
| SC.L2-3.13.8 | <b>Data in Transit</b><br>Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.   | ✓         |



## System and Communications Protection (SC)

| CMMC 2.0      | Details   | FileCloud |
|---------------|---|-----------|
| Level 2       |   |           |
| SC.L2-3.13.9  | <b>Connections Termination</b><br>Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.   | N/A       |
| SC.L2-3.13.10 | <b>Key Management</b><br>Establish and manage cryptographic keys for cryptography employed in organizational systems.   | ✓         |
| SC.L2-3.13.11 | <b>CUI Encryption</b><br>Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.  | ✓         |
| SC.L2-3.13.12 | <b>Collaborative Device Control</b><br>Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. | N/A       |
| SC.L2-3.13.13 | <b>Mobile Code</b><br>Control and monitor the use of mobile code.   | N/A       |
| SC.L2-3.13.14 | <b>Voice over Internet Protocol</b><br>Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.   | N/A       |





## System and Communications Protection (SC)

| CMMC 2.0      | Details  | FileCloud |
|---------------|--|-----------|
| Level 2       |  |           |
| SC.L2-3.13.15 | <b>Communications Authenticity</b><br>Protect the authenticity of communications sessions. | N/A       |
| SC.L2-3.13.16 | <b>Data at Rest</b><br>Protect the confidentiality of CUI at rest.                         | ✓         |

## System and Information Integrity (SI)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 1      |  |           |
| SI.L1-3.14.1 | <b>Flaw Remediation</b><br>Identify, report, and correct information and information system flaws in a timely manner.                          | N/A       |
| SI.L1-3.14.2 | <b>Malicious Code Protection</b><br>Provide protection from malicious code at appropriate locations within organizational information systems. | N/A       |



# System and Information Integrity (SI)

| CMMC 2.0     | Details  | FileCloud |
|--------------|--|-----------|
| Level 1      |  |           |
| SI.L1-3.14.4 | <b>Update Malicious Code Protection</b><br>Update malicious code protection mechanisms when new releases are available.  | N/A       |
| SI.L1-3.14.5 | <b>System &amp; File Scanning</b><br>Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.     | N/A       |
| Level 2      |  |           |
| SI.L2-3.14.3 | <b>Security Alerts &amp; Advisories</b><br>Monitor system security alerts and advisories and take action in response.  | N/A       |
| SI.L2-3.14.6 | <b>Monitor Communications for Attacks</b><br>Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | N/A       |
| SI.L2-3.14.7 | <b>Identify Unauthorized Use</b><br>Identify unauthorized use of organizational systems.   | N/A       |



## Learn More

To learn more about cybersecurity, click the links below.

[How to Make Organizations Cyber Resilient in the Digital Frontier →](#)

[The Hidden Costs of Cybercrime →](#)

[About the CMMC →](#)

[The Evolution of FAR 52.204-21 to CMMC →](#)

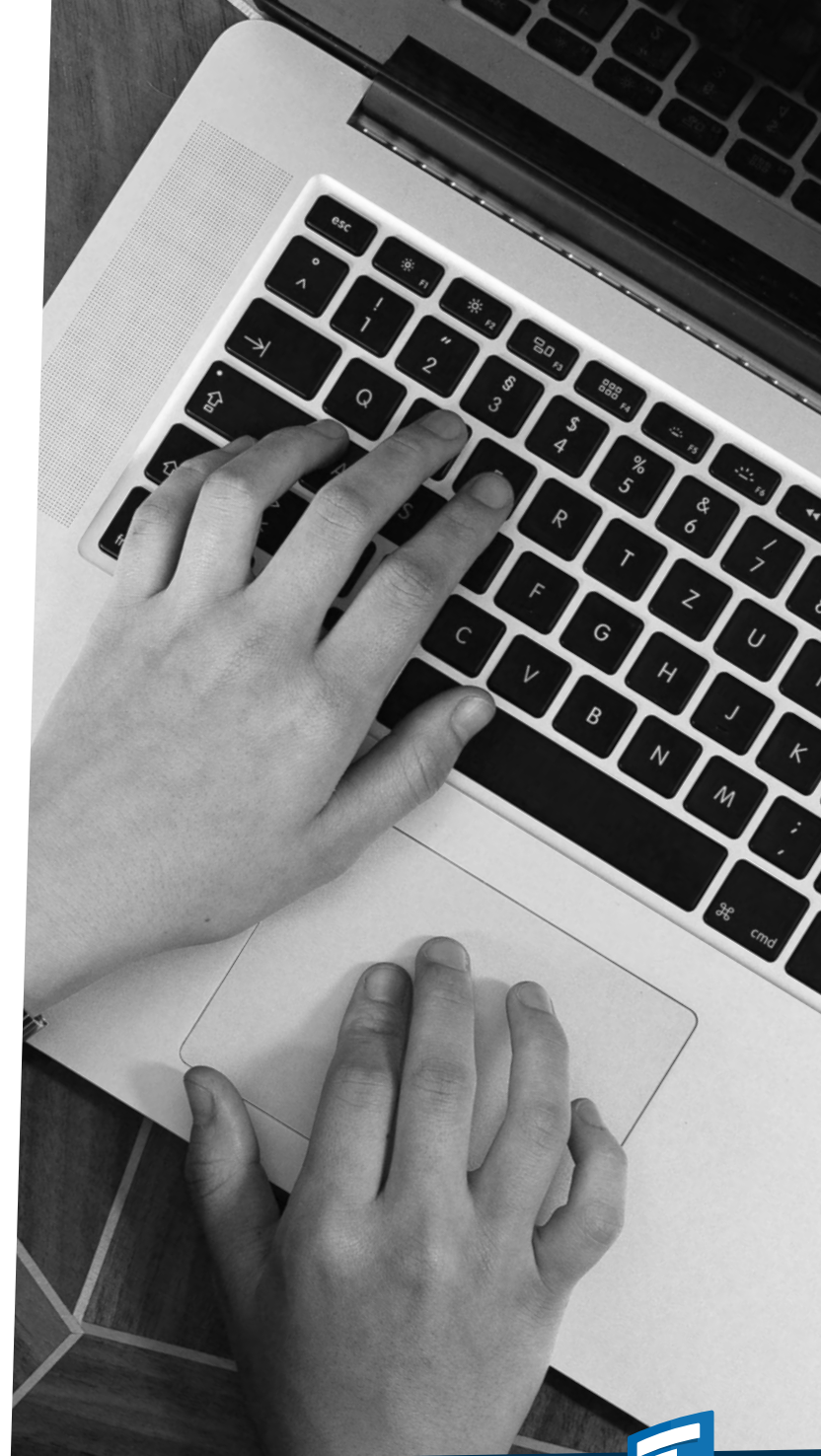
[Cybersecurity Maturity Model Certification \(CMMC\) 2.0 Updates and Way Forward →](#)

[CMMC 2.0 could take as long as two years to come online →](#)

[Proposed Rule, Cybersecurity Maturity Model Certification \(CMMC\) Program →](#)

[Pentagon reveals updated cost estimates for CMMC implementation →](#)

[CMMC Documentation →](#)



## Glossary of Terms

(in order of appearance)

**CMMC:** Cybersecurity Maturity Model Certification

**DIB:** Defense Industrial Base

**DoD:** Department of Defense

**FCI:** Federal Contract Information

**CUI:** Controlled Unclassified Information

**OSD(A&S):** Office of the Under Secretary of Defense for Acquisition and Sustainment

**UARC:** University Affiliated Research Centers

**FFRDC:** Federally Funded Research and Development Centers

**FAR:** Federal Acquisition Regulation

**DFARS:** Defense Federal Acquisition Regulation Supplement

**NIST:** National Institute of Standards of Technology

**SP:** Special Publication

**SPRS:** Supplier Performance Risk System

**DIBCAC:** Defense Industrial Base Cybersecurity Assessment Center

**ANPRM:** Advance Notice of Proposed Rulemaking

**CFR:** Code of Federal Regulations

**OMB:** Office of Management and Budget

**C3PAO:** Certified Third-Party Assessor Organization



## About Us

FileCloud is a hyper-secure file sharing, collaboration, and governance solution that provides industry-leading tools for compliance, data leak protection, data retention, and digital rights management. Workflow automation and granular control of content sharing are fully integrated into the complete feature stack.

The FileCloud platform offers powerful file sharing, sync, and mobile access capabilities on public, private, and hybrid clouds. Headquartered in Austin, Texas, FileCloud is deployed by top Global 1000 enterprises, educational institutions, government organizations, and managed service providers, with over one million users worldwide.



**1M+**  
USERS



**3000+**  
ENTERPRISES



**100+**  
RESELLERS



**90+**  
COUNTRIES



13785 Research Blvd, Suite 125  
Austin TX 78750, USA

**Phone:** U.S: +1 (888) 571-6480

**Fax:** +1 (866) 824-9584

**CONTACT US**



US Army Corps  
of Engineers



**Deloitte.**



## Copyright Notice

© 2024 FileCloud. All rights reserved.  
No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

