VisibleThread

VISIBLETHREAD GUIDE

CMMC, FedRAMP and equivalency

What federal contractors actually need to know

A plain English guide to the two frameworks, the route called equivalency, and how to pick a deployment that fits your assessment.

Drawn from the VisibleThread webinar with Ignyte, September 2026

THE LANDSCAPE

Two frameworks, two different jobs

CMMC and FedRAMP get used interchangeably and they are not the same thing. One governs your systems. The other governs the cloud products you put your data into. There is no formal reciprocity between them.

	CMMC	FedRAMP
Covers	Contractor information systems	Cloud service offerings
Governed by	Department of Defense	General Services Administration
Measured against	NIST SP 800-171	NIST SP 800-53
Assessed by	C3PAO or DIBCAC	3PAO

DoD guidance keeps NIST SP 800-171 Rev. 2 as the contractually referenced version for CMMC assessments, even though Rev. 3 has been published.

You put CUI into a cloud tool. That tool needs FedRAMP Moderate equivalency or higher.	You connect a service that your CUI flows into. Same requirement applies to it.	You create, process or store CUI in your own environment. You are in CMMC scope.

The July pause does not change the cloud requirement

CMMC Phase 2 was suspended in July 2026. The pause covers the assessment requirement, meaning Level 2 C3PAO assessments and Level 3 government assessments, while the reform task force does its review. DFARS 252.204-7012, Phase 1 self assessments, SPRS submission, annual affirmations and subcontractor flow down all continue. The cloud provider requirement was not part of the pause.

VisibleThread

EQUIVALENCY

The route that exists because most providers have no agency sponsor

A FedRAMP authorization needs a sponsoring agency. Most cloud providers cannot get one, and DoD still needs cloud products. So DoD published a memo creating equivalency, a route where a provider is assessed against the FedRAMP Moderate baseline and hands the evidence to the customer instead of to an agency.

Ready	Authorized	Equivalent
A 3PAO assessed the provider's readiness and the FedRAMP PMO agreed. It is a readiness designation. It is not an authorization and it is not equivalency.	An agency sponsor, a completed full assessment, and an agency official who formally accepts the residual risk. This is an ATO.	A full assessment against the FedRAMP Moderate baseline by a FedRAMP recognized 3PAO, with the body of evidence given to the customer under NDA. No agency sponsor involved.

> **Under equivalency there is no agency official who can accept risk, so findings cannot stay open. They have to be closed, and the 3PAO has to validate the closure, before the assertion stands.**

WHAT THE BODY OF EVIDENCE CONTAINS

- System Security Plan
- Security assessment plan
- Assessment report
- Customer responsibility matrix
- Continuous monitoring evidence

FedRAMP restructured in summer 2026 and the impact levels became certification classes, with Moderate now Class C. The equivalency requirement comes from the DoD memo, which names the FedRAMP Moderate baseline, so that remains the baseline for assessment. Some providers now write "FedRAMP Moderate / Class C" to cover both.

WHERE YOUR CUI LIVES

Four ways to run VisibleThread

The question is whose assessment the system sits inside, not which option is more secure.

Customer hosted: on premises

Built for SCIFs and air gapped environments

Installs on Windows or Red Hat including bare metal, fully customer managed, complete data sovereignty.

Sits inside your CMMC boundary. Assessed with your environment.

Customer hosted: private cloud

Built for regulated industries

Deployable to Azure GCC High, AWS FedRAMP environments and private data centres, with dedicated resources and full administrative control.

Sits inside your CMMC boundary. Assessed with your environment.

US GovCloud: single tenant

Hosted by VisibleThread

In AWS GovCloud (US). A dedicated single tenant environment per customer, US persons support, FIPS 140-2/140-3 validated encryption for all data and communications. This is the deployment going through equivalency.

Sits inside VisibleThread's assessment. Your assessor reviews our evidence.

Public cloud: multi tenant

For teams doing no regulated work

Instant access, no setup or maintenance, managed updates and high availability.

Not for CUI.

Moving between deployments is supported and we have done it many times. If you went customer hosted years ago because our cloud was not an option, you can move.

Same platform wherever it runs. VisibleThread 7.3 is available across all four deployments, with ownership and collaboration, customisable stage gates, full auditability, and generated output that traces back to the source requirement.

WHERE WE ARE

Our position today

1

FedRAMP Ready, granted by the FedRAMP PMO on 7 July 2026. Listed on the FedRAMP Marketplace.

2

Full assessment underway with our 3PAO, Ignyte, who are also a CMMC assessor.

3

On attestation we assert DoD FedRAMP Moderate equivalency, and the body of evidence goes to customers under NDA.

Status correct as of 16 September 2026

QUESTIONS WE GET ASKED

We are already in AWS GovCloud or GCC High. Does that make us compliant?	No. Authorization of the infrastructure covers the infrastructure. The service running on top of it has to be assessed separately. That includes us, which is why we run our own assessment rather than relying on AWS.
Everyone says FedRAMP equivalent. Why should I believe yours?	You do not have to take our word for it. Under NDA you receive the System Security Plan, assessment plan, assessment report, customer responsibility matrix and supporting evidence, and your assessor reviews it. That is the mechanism the DoD memo sets up. Under equivalency, findings cannot stay open.
If I host it myself, what does that do to my CMMC assessment?	VisibleThread becomes a component of your environment, so it sits in your boundary and is assessed by your C3PAO at every assessment. With our GovCloud offering your assessor reviews our evidence instead. The requirement is the same either way. The difference is where the work happens.
Who at VisibleThread can touch my data?	In the GovCloud environment access to customer data is restricted to US persons, enforced by screening and by technical access restrictions. Each customer has a dedicated single tenant environment. Access requires phishing-resistant MFA and everything is logged.
Where does my content go when I use the AI features?	In the GovCloud environment the AI capability runs on AWS's managed AI service, inside the same GovCloud boundary as the rest of the deployment. Content does not leave that boundary for a third party model provider, and it is not used to train models.

Questions about your own deployment, or about the evidence package? Talk to your VisibleThread customer success manager or book a technical session.

Thanks to Christina M. Martinson and the team at Ignyte, our 3PAO, for the compliance detail in this guide.