CYBERSHEATH

GCC Guide

What You Need to Know About Microsoft 365 Government Community Cloud and CMMC Compliance

As a DOD contractor, Microsoft 365 Government Community Cloud (GCC) and Microsoft 365 Government Community Cloud High (GCC High) can play a large role in helping your organization secure Controlled Unclassified Information (CUI) and meet the requirements of DFARS 252.204-7012 (DFARS) and CMMC. But what are these offerings, which version do you need, and how do you avoid buying unnecessary software licenses?

CyberSheath is a certified Microsoft 365 reseller. We know the capabilities of Microsoft Office 365 as the go-to software platform for data security and understand that it is just one piece of the compliance puzzle you are working to solve. This guide helps you make an informed decision before you purchase any Licenses by explaining the product tiers, clarifying which level fits your requirements, and outlining why licensing alone does not deliver full compliance.

What is Microsoft 365 GCC?

Microsoft 365 GCC is a U.S. government cloud community derived from Microsoft 365 Commercial and tailored for organizations that handle sensitive government data.
It comes in two tiers.

- **Microsoft 365 GCC** - Often shortened to GCC, this environment provides many of the same productivity and collaboration capabilities as Microsoft 365 Commercial (Exchange, SharePoint, OneDrive, Teams, etc.), but in an environment aligned to FedRAMP Moderate requirements. For organizations pursuing DFARS/CMMC objectives, GCC can be configured and governed to support implementation of NIST SP 800-171 controls, enabling an organization to store, process, and transmit CUI in a compliant manner. GCC also allows organizations to leverage Microsoft's cloud security capabilities (e.g., identity protection, threat detection, audit/logging, and compliance tooling) built on Azure.

- **Microsoft 365 GCC High** - Microsoft's U.S. Sovereign cloud environment for U.S. government customers and qualifying organizations with requirements beyond commercial or GCC. It is hosted in U.S. datacenters, physically and logically separated from Microsoft's commercial cloud, and includes U.S. data residency with U.S.-person–restricted operations/administration. GCC High delivers Microsoft 365 collaboration services and, with appropriate configuration and governance, can support NIST SP 800-171 and DFARS/CMMC objectives for handling CUI. It's often selected when contract or regulatory obligations (including ITAR/EAR-related expectations) require tighter control over where data resides and who can administer the environment.

How do you know what you need?

Microsoft 365 licensing can be a significant budget item, and the right environment is not always the highest tier. It should match your contract language, the data you handle (e.g., CUI vs. export-controlled), and how your tenant and administrative model are structured. Our goal is to help you select licensing that meets your operational and regulatory requirements without overspending unnecessarily or choosing an option that still leaves gaps in compliance.

Standard	Data Type	Primary Requirements	Recommended Microsoft Environment
CMMC 2.0 Level 1	Federal Contract Information (FCI)	17 basic cybersecurity hygiene practices	Microsoft 365 Commercial
CMMC 2.0 Level 2	CUI	110 NIST SP 800-171 controls	GCC or GCC High
DFARS 7012	CUI	110 NIST SP 800-171 controls + incident reporting	GCC or GCC High (depending on contract requirements)
ITAR	Export-controlled data	Sovereign cloud; U.S. Persons only	GCC High (mandatory)

The chart above is a helpful starting point, but selecting the right environment is a business decision as much as a technical one. An expert review of your contracts, data, and current environment is the best way to determine what you need in detail. The right compliance solution fits your organization and the way it operates in order to avoid overspending and under-complying.

Software isn't enough

A FedRAMP compliant collaboration platform such as Microsoft GCC or GCC High is a tool, not a comprehensive compliance solution. Full DFARS and CMMC readiness requires implementing all 110 NIST SP 800-171 requirements. While these platforms provide technical capabilities that can support many of these controls, compliance largely depends on governance, documentation, and operational discipline.

- Choosing GCC High when standard GCC meets your requirements can add unnecessary licensing costs and operational complexity without improving your overall compliance outcomes. It's also important to remember that licensing alone does not close common compliance gaps, such as: Written policies and procedures required under NIST 800-171
- Continuous network monitoring and audit log review
- Incident response planning and tabletop exercises
- System Security Plan (SSP) and Plan of Action and Milestones (POAM) documentation
- Access control management, user training, and physical security requirements

How to spot a software-first vendor

Many providers in this space focus primarily on selling licenses. A common red flag is when the first recommendation is to purchase GCC High licensing, often before anyone has reviewed your environment, and discussed your data types and contract requirements. They will talk about getting you to compliance, but many lack the depth of experience to deliver it.

A compliance-first provider starts with a conversation. They evaluate how you operate, what your agreements require, what gaps exist today, then recommend the right environment and controls. Software selection follows the assessment—it does not precede it.

Overview of the Microsoft Government Cloud Platforms

As you strengthen your security posture and work toward NIST SP 800-171 compliance and CMMC Level 2 certification, Microsoft 365 can provide both a secure foundation and the collaboration tools teams rely on every day. With built-in capabilities for identity, auditing, and data protection, organizations can improve security while also streamlining day-to-day operations through familiar Office apps, email, file sharing, and Teams-based collaboration.

Microsoft 365 is available in several FedRAMP authorized environments, each with different hosting boundaries and operational requirements. Understanding the practical differences between them helps you choose the right fit for your contract obligations, the data you handle, and your day-to-day workflows.

Office 365 GCC / Azure Commercial / Dynamics 365 Government

GCC originated as a dedicated segment of Microsoft's commercial cloud, purpose-built to serve state and local government, federal civilian agencies, and the defense industrial base (DIB). It uses Azure Commercial as its underlying platform and aligns with FedRAMP Moderate authorization while supporting organizations implementing DFARS 252.204-7012 and NIST SP 800-171 security requirements.

For DIB contractors whose work does not involve export-controlled data, GCC is generally sufficient to support CMMC Levels 1 and 2. Note that the environment shares underlying infrastructure with Azure Commercial, which is a globally distributed platform, and therefore does not satisfy the data sovereignty requirements associated with most export-controlled CUI categories.

Office 365 GCC High / Azure Government / Dynamics 365 GCC High

GCC High is Microsoft's government cloud environment for eligible U.S. government agencies and qualifying Defense Industrial Base organizations that require U.S.-based hosting, U.S. data residency, and U.S.-person–restricted operations and administration. It

is architecturally separated from Microsoft's commercial cloud at the network and data layers, and it aligns with DISA SRG Impact Level 4 requirements.

GCC High delivers the core Microsoft 365 collaboration services and includes Microsoft's security and compliance capabilities within the same environment. This includes Entra for identity and access management, Defender for threat protection, Purview for data governance and compliance, and Sentinel for SIEM and security analytics.

For defense contractors, GCC High is often used to support DFARS 252.204-7012 and CMMC Level 2 compliance efforts, and it is frequently selected for ITAR, EAR, and other export-controlled workloads that require tighter controls over where data resides and who can access or administer the platform. GCC High is built on Azure Government infrastructure, which also underpins DOD cloud services.

Office 365 DOD / Azure Government / Dynamics 365 DOD

These DOD environments are purpose-built for the U.S. Department of Defense and are not generally available to the Defense Industrial Base. Microsoft's guidance is straightforward: if you are not part of the DOD, you should not plan on using these services. Access to Microsoft 365 DOD and the DOD regions for Azure is limited to DOD customers and organizations explicitly approved by the DOD, such as authorized service providers or mission partners operating under DOD authorization.

Other Microsoft Government Environments

Microsoft also offers additional environments for eligible U.S. government customers supporting classified workloads with more restrictive security requirements. Azure Government Secret is intended for U.S. government classified workloads and is authorized for DOD use under DISA SRG Impact Level 6. Azure Government Top Secret supports highly sensitive national security missions and is available only to approved U.S. government customers with the required authorizations.

Microsoft continues to evolve its government cloud offerings and partner ecosystem to better support CMMC-related requirements, including expanding capabilities and working toward greater feature parity with the commercial Microsoft 365 platform across government environments. CyberSheath is a Microsoft Cloud Solutions Provider and Microsoft Premier Support partner, and is also among a select group of authorized resellers for Microsoft 365 GCC High and Microsoft 365 GCC licensing.

Consider an enclave approach

An enclave is a strategically segregated architecture used to reduce compliance scope by isolating where CUI or export-controlled data is stored, processed, and accessed. Rather than moving your entire organization into GCC or GCC High, you create a dedicated, tightly controlled environment

for the specific users and workflows that handle CUI or ITAR data. This approach is common across DIB contractors of all sizes because it aligns security and compliance efforts to the organization's actual CUI footprint, often improving cost efficiency while keeping the rest of the business on standard commercial platforms and tooling.

How it works

In an enclave model, your company operates in two distinct environments.

- **Commercial:** All staff remain in your existing Microsoft 365 commercial tenant for everyday business (Sales, Marketing, HR, Engineering, Manufacturing, Field Staff, Shop Floor, etc.) using standard commercial licenses.
- **CMMC Compliant Cloud Enclave - GCC/GCC High:** Only the users and workflows that store, process, or transmit CUI, or handle export-controlled work, use a separate tenant with tighter security and operational requirements. Enclave users typically have a second identity in this tenant in addition to their commercial account.

If you are considering an enclave approach, give us a call. We can guide you through scoping, design, and implementation to help protect CUI and support your NIST SP 800-171, and DFARS 252.204-7012 requirements to get you CMMC L2 certified. You can also learn more in our CUI Enclave Guide.

Frequently Asked Questions About GCC and GCC High

1. **What is the difference between GCC and GCC High?**

   GCC aligns with FedRAMP Moderate controls and can support organizations implementing DFARS 252.204-7012 requirements. It is appropriate for most contractors working with CUI who do not handle export-controlled data. GCC High is Microsoft's fully U.S. sovereign cloud, and is required when your contracts involve ITAR, EAR, or other export-controlled CUI categories.

2. **Will buying GCC or GCC High make me CMMC compliant?**

   No, GCC and GCC High are tools that can help you implement and operate required controls, but they are not compliance solutions by themselves. Software is the starting point—not the finish line. CMMC Level 2 readiness requires the right configurations plus documented policies, procedures, evidence, and ongoing security operations, not just a license.

3. **How do I know which GCC tier my contract requires?**

   Your contract language and the type of CUI you handle are the determining factors. Review your DFARS clauses, any ITAR or EAR obligations, and the specific CUI categories identified in your contract.

4. **Can I migrate from GCC to GCC High later if my requirements change?**

   Yes, but it is a tenant-to-tenant migration, not a simple upgrade. Moving to GCC High involves migrating users, mail and files, reconfiguring applications and security settings, updating integrations, and revising your SSP and related compliance documentation. It takes planning, time, and resources, so it's best to choose the right environment up front when possible.

5. **Can my team still collaborate with people outside of GCC High?**

   Yes. In GCC High, external collaboration is often more restricted by default than in commercial Microsoft 365, but it can be configured to support guest access and secure sharing where appropriate. Working with an experienced partner can make the difference between enabling cross-organization collaboration in a way that supports your compliance requirements and unintentionally weakening your security boundary.

6. **Does CyberSheath sell GCC and GCC High licenses?**

   Yes. CyberSheath is one of a select group of Microsoft-authorized resellers eligible to provide Office 365 GCC and GCC High licensing (AOS-G and GCC High License Eligible). Unlike license-first vendors that recommend GCC High before reviewing your data types, and environment, we take a requirements first approach. We recommend the licensing and configuration that meets your needs without unnecessary spending or avoidable compliance gaps.

Resources

- For a detailed breakdown of all Microsoft government cloud environments, including GCC, GCC High, Office 365 DOD, Azure Government, and Secret/Top Secret offerings, refer to Microsoft's official breakdown on the Tech Community blog.
- Check out CyberSheath's CUI Guide for what you need to know about Controlled Unclassified Information.
- Refer to CyberSheath's CUI Enclave Guide to get started on establishing an enclave to protect your CUI.

Talk to the Experts

Before you buy a single license, talk to a compliance expert. The cost of the wrong decision—overpaying for licenses you don't need, or under-complying with the requirements you have—is far greater than the cost of getting it right from the start.

CyberSheath offers a no-cost, no-obligation initial conversation to help you understand what you actually need. Contact us today to learn more.