mission multiplier

Why Taking an "Enclave" Approach is Optimal for Achieving CMMC Compliance

Why the "Leading CMMC Compliance Solution" for encrypted email & file sharing (while good) does not cover the bases when it comes to achieving full compliance

September 2025

1.0 INTRODUCTION

As CMMC 2.0 Level 2 assessments continue to accelerate across the Defense Industrial Base (DIB), as contractors are seeking turnkey solutions that promise ease of deployment and cost-efficiency. Although the "Leading CMMC Compliance Solution" for encrypted email & file sharing is a secure collaboration platform that has been marketed as a standalone, compliant solution for meeting CMMC Level 2 requirements, it does not fully meet all the required compliance requirements.

The CMMC acquisition rule (48 CFR) was submitted to the Office of Information and Regulatory Affairs (OIRA) for review in late July 2025, and its formal enactment to implement CMMC requirements into DoD contracts is expected in late 2025, with phased contract inclusion through 2028. While the overarching CMMC program rule (32 CFR) became effective on December 16, 2024, the 48 CFR rule is required to enable contracting officers to include CMMC requirements in solicitations.

In contrast, many DIB contractors are turning to a Microsoft Azure Government (GCC) "Enclave Solution" as the fastest and most effective way to achieve and maintain compliance with NIST SP 800-171 and CMMC Level 2 requirements. This is the solution that Mission Multiplier specializes in implementing, in order to realize the following key benefits:

- **Aligned to NIST SP 800-171 & CMMC**: Microsoft GCC is specifically engineered to support the 110 practices in NIST SP 800-171. Microsoft provides control inheritance documentation, so contractors know which security requirements are already covered by the platform. This reduces effort and accelerates compliance.
- **Controlled Access to CUI**: By isolating Controlled Unclassified Information (CUI) within a GCC enclave, contractors demonstrate clear separation from non-compliant systems. This minimizes audit scope, reduces risk, and lowers overall assessment costs.
- **Enhanced Security & Monitoring**: With integrated tools like Microsoft Purview, Defender, Sentinel, and Intune, GCC provides full-spectrum monitoring, logging, and endpoint protection. Contractors gain end-to-end visibility and the ability to implement continuous monitoring for sustained compliance.
- **Federal-Grade Infrastructure**: GCC runs in US-only data centers staffed by background-checked US citizens. It meets FedRAMP High and DoD SRG Impact Level 4/5 authorizations, ensuring data residency and handling align with federal standards.
- **Scalable & Cost-Effective**: Instead of migrating entire infrastructures, contractors can establish enclave environments for sensitive workloads. This targeted approach reduces costs and complexity while enabling compliance.
- **Audit-Ready & Evidence-Based**: GCC integrates seamlessly with Governance, Risk, and Compliance (GRC) tools such as IntelliGRC. Logs, policies, and configurations can be automatically exported as evidence, reducing audit timelines and ensuring assessor confidence.

By adopting a Microsoft GCC enclave, Mission Multiplier helps government contractors achieve compliance with the CMMC Level 2 standard by using an "Enclave Approach" because it is cost effective, can scale as needed, and can be implemented successfully in as soon as two to three weeks. We also **guarantee that you will pass your audit**, if you adhere to our guidance.

2.0 CYBERSECRUITY MATURITY MODEL CERTIFICATION (CMMC) OVERVIEW

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is the Department of Defense's streamlined framework for protecting sensitive government information across the Defense Industrial Base (DIB). Introduced in November 2021 as an update to the original CMMC 1.0 model, CMMC 2.0 simplifies requirements, aligns closely with existing federal cybersecurity standards, and provides a more flexible path for organizations, especially small and mid-sized businesses—to achieve and maintain compliance.

At its core, CMMC 2.0 aims to:

- Safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).
- Enhance trust across the DoD supply chain by ensuring consistent cybersecurity practices.
- Balance security with practicality, reducing compliance costs while still addressing cyber threats.
- Enable the use of Plans of Action & Milestones (POA&Ms) to close gaps, while introducing stronger enforcement through annual affirmations and government-led oversight.

"LEADING SOLUTION" STANDALONE APPROACH

The "Leading CMMC Compliance Solution" for encrypted email & file sharing is a secure email and file sharing platform advertised as CMMC-friendly. While This solution offers end-to-end encryption and FedRAMP Moderate hosting, it does not natively support full CMMC implementation (e.g., required functionality like endpoint protection, centralized logging, vulnerability management, etc.).

Fundamentally, the "Leading Solution" is a secure file-sharing and messaging platform, and although it is advertised as "CMMC-compliant" and "easy to implement," it is solely focused on encryption, access control, and data sovereignty. While it is a great solution for what it does, it does not achieve full CMMC compliance.

Here are the benefits that the "Leading Solution" provides:

- End-to-end encryption with user-managed keys
- Email and file sharing that meets DFARS 7012
- Zero-trust architecture
- FedRAMP-moderate infrastructure

Below is a breakdown of what it provides and doesn't provide when it comes to CMMC compliance by both CMMC Domain, as well as by additional need functional capability.

CMMC Domain	Coverage with the "Leading Solution"
Access Control	Partial (user-side enforcement)
Audit & Accountability	Limited (no native centralized SIEM or long-term logging)
Incident Response	Not included
Configuration Management	Not applicable (hosted SaaS only)
Identification & Authentication	Partial (no control over ID provider)
Risk Assessment	Not provided
Device Management	Not included
Vulnerability Management	Not included
Security Awareness Training	Not included

Requirement	Additional Tools / Services Needed
Logging/SIEM	Sentinel, Splunk, or third-party solution
EDR	Defender for Endpoint, CrowdStrike, SentinelOne
System Security Plan	Custom development and documentation
Mobile Device/Endpoint Management	Intune, JAMF, etc.
Asset Management	Manual or commercial solutions
Incident Response Procedures	Internal development
Policy Framework	Internal or third-party development

Based on this understanding, it is essential that the "Leading Solution" be combined with other solutions or services to ensure full compliance.

COST BREAKDOWN – The "Leading Solution" vs. Enclave Approach

The following table outlines estimated costs to fill the gaps of the "Leading Solution" (assuming 3 users).

Required Component	Estimated Monthly Cost (USD)	Estimated One-Time Cost (USD)
"Leading Solution" Platform	$200	
Endpoint Detection & Response (EDR)	$500	
Mobile Device Management (MDM)	$300	
SIEM/Security Logging	$1,000	
Policy Framework & Documentation		$5,000
Incident Response Plan & Testing		$5,000
User Access Review/Management	$250	
Vulnerability Management	$400	
CMMC Implementation Consultant*		$25,000
Annual Compliance Support Services	$1,500	
GCC License	$200	
GRC Tool		$5,000
C3PAO Audit		$50,000**
Total	*$4,350.00 (Monthly)* *$49,800.00 (Annual)*	$90,000 (One-time)

*Cost to develop documentation and capture all audit artifacts in GRC solution, as well as real-time audit support
**Cost every 3 years

The following table outlines estimated costs taking the GCC Enclave Approach (assuming 3 users).

Required Component	Estimated Monthly Cost (USD)	Estimated One-Time Cost (USD)
Endpoint Detection & Response (EDR)		
Mobile Device Management (MDM)		
SIEM/Security Logging		
Policy Framework & Documentation		
Incident Response Plan & Testing	$1,250.00	
User Access Review/Management		
Vulnerability Management		
CMMC Implementation Consultant*		
Annual Compliance Support Services		
GCC License	$180	

Virtual Machines	$180	
GRC Tool		$5,000
C3PAO Audit		$30,000***
Total	*$1,330.00 (Monthly)*	$35,000

**Mission Multiplier possesses a strategic partnership with Kieri, a certified C3PAO, that offers us significantly discounted pricing for our audits based on our innovative and streamlined approach.

7.0 The Solution Provider

Mission Multiplier is a certified small business headquartered in Huntsville, Alabama that specializes in full spectrum cybersecurity solutions – with a focus on cyber services for government and commercial markets, as well as the development of innovative tools and technologies. We are considered experts in the areas of CMMC and cyber compliance. In fact, we are one of a few organizations that have developed and successfully implemented a "audit passing" GCC Enclave approach.

Mission Multiplier was founded on a truly innovative business value proposition. For every hour a Mission Multiplier employee works, we direct a portion of the company profit to a local charity of the employee's choice. In this way, each employee knows that not only are they getting to develop and deliver innovative cybersecurity services, but that they are directly giving back to the local community. Building on this principle, our goal is to multiply the successes that our clients achieve against their respective missions, while simultaneously enabling the missions of our employees – with the result of securing and enriching the communities we serve.

Mission Multiplier
1300 Meridian St N Suite 101 Huntsville, AL 35801
www.missionmultiplier.com