# TEHAMA DATA ENCLAVES

## CMMC Acceleration for the Defense-Industrial Base

Whitepaper

January 2026

# Executive Summary

In the face of escalating nation-state threats, defense contractors and organizations within the Defense Industrial Base (DIB) are under immense pressure to safeguard Controlled Unclassified Information (CUI). Compliance is no longer a paperwork exercise; stringent standards like the **Cybersecurity Maturity Model Certification (CMMC)** now demand demonstrable, evidence-based governance down to the workload level.

This white paper examines the critical challenges DIB organizations face in achieving **NIST SP 800-171** compliance. It exposes how traditional "patchwork" solutions—VPNs, legacy VDI, and shipping physical laptops—create sprawling attack surfaces that are prohibitively expensive to audit and defend.

We present a fundamental shift in strategy: **Tehama Technologies' Self-Custody Data Enclaves.**

This architecture empowers organizations to deploy a "Clean Room" for CUI directly within their own cloud tenancy (Azure or AWS). By doing so, organizations retain exclusive ownership of encryption keys, audit logs, and identity management, ensuring Tehama maintains zero actual access to sensitive workloads. This approach allows defense contractors to inherit the massive compliance investments of hyperscalers, significantly reduce their assessment scope, and accelerate certification without sacrificing operational agility.

The objective of this white paper is to provide DIB organizations with a blueprint for **sovereign compliance.** We detail how Tehama's pre-configured controls map directly to NIST 800-171 requirements—enforcing strict access policies, automating audit evidence, and establishing a defensible perimeter that dramatically reduces the time, cost, and risk of achieving CMMC Level 2readiness.

> Beyond regulatory alignment, Self-Custody Data Enclaves deliver measurable business value. By reducing compliance scope and automating audit evidence, organizations can shorten assessment timelines, lower audit and engineering costs, and reduce operational risk. This approach also enables faster onboarding of subcontractors and partners, improves readiness for contract awards, and supports secure adoption of emerging technologies such as AI, without expanding compliance burden.

# Introduction

Organizations within the Defense Industrial Base (DIB) must reconcile two opposing forces: the operational need for advanced, data-driven collaboration and the regulatory imperative to strictly isolate and secure Controlled Unclassified Information (CUI).

As cyber threats evolve into sophisticated campaigns targeting the supply chain, the regulatory bar has been raised. Self-attestation is being replaced by third-party assessments (C3PAOs) under **CMMC**. In this new era, traditional security models—including Desktop-as-a-Service (DaaS), Virtual Private Networks (VPNs), Identity & Access Management (IAM), and unmanaged endpoints—are proving insufficient. They create fragmented environments that are overly complex to manage and too porous to pass a rigid compliance audit.

To address these mission-critical challenges, Tehama Technologies pioneered the **Secure Data Enclave**. This next-generation solution is purpose-built to accelerate and simplify compliance for the DIB. A Tehama Enclave acts as an air-gapped digital vault, isolating critical workloads and CUI from the rest of the corporate network. This "segmentation by design" establishes a compliant, defensible perimeter that enforces Zero Trust access policies while preventing data leakage.

Crucially, this paper introduces Tehama's **Self-Custody** deployment option. Unlike traditional SaaS models that require you to trust a vendor with your data, Self-Custody places the enclave entirely within your own cloud tenant. This ensures that you alone hold the keys to the kingdom—controlling identity, encryption, and audit logs—while Tehama operates the control plane with zero access to your sensitive defense information.

This white paper details how Tehama's data enclaves deliver:

- **Scope Reduction:** Removing corporate networks and endpoints from the assessment scope by isolating CUI within a secure boundary.
- **Inherited Compliance:** Leveraging the physical security and FIPS-validated cryptography of Azure and AWS to satisfy NIST 800-171 controls automatically.
- **Operational Agility:** Enabling the secure integration of emerging technologies like Artificial Intelligence (AI) within a governed sandbox, allowing DIB organizations to innovate without compromising security.

By moving beyond legacy infrastructure to a Sovereign Enclave strategy, defense contractors can achieve compliance not as a burden, but as a scalable competitive advantage.

# Table of Contents