// PRECISION MANUFACTURING

Doubling in Size Without Redrawing the Compliance Boundary

A small shop with the majority of its revenue tied to Department of Defense contracts, a CMMC deadline it did not set, and a GCC High migration it could not afford. Reaching audit-ready without the migration — and without the boundary ever moving again.

TUSA-CASE-002 · V1.0 · 11 SEPTEMBER 2026 · PUBLIC · TRANUSA, LLC

Client profile. A small custom metal fabrication, CNC machining and laser processing shop in the Midwest, with the majority of its revenue tied to Department of Defense contracts.

Client name and identifying details have been withheld or generalized to protect confidentiality, consistent with TRANUSA's practice across all client engagements.

110/110	2×	FIPS 140-2	Audit-Ready
SPRS self-assessment score	Headcount growth, boundary unchanged	Certified network hardware	Evidence locker maintained

01 The Problem

The shop's contracts depended on CMMC Level 2, and the timeline was not theirs to set. With the majority of revenue tied to DoD work, the requirement was a business problem before it was a security one. As a small shop they had no internal team to build the controls, and anything that worked had to fit inside the infrastructure and the budget they already had.

The obvious path was expensive. Meeting the requirement conventionally starts by moving the organization into Microsoft 365 GCC High, and for a shop this size that migration was both cost-prohibitive and disruptive to production. It was harder then than it would be now: Microsoft had not yet released the GCC High Business Premium tiers that have since brought that cost down. Doing it the standard way meant spending heavily and interrupting the work that pays for everything.

They were running Microsoft 365 Commercial across the organization and had begun looking at PreVeil as a place to handle controlled data — the right instinct, scoped to the three people who touched CUI directly.

02 What TRANUSA Did

TRANUSA came to the engagement through a referral: a colleague of the client's CTO recommended us. The CTO then vetted TRANUSA against other MSSPs working in this space before anything was signed. The work was earned on a recommendation and tested on the merits.

Leaving them where they were

The first decision was not to migrate. Rather than moving to GCC High, TRANUSA built the CUI enclave in PreVeil alongside their existing Microsoft 365 Commercial tenant. That met the requirement without the licensing cost of a migration and without taking production offline to do it.

How wide to draw it

The client's plan was a three-seat enclave covering the people who handled CUI directly. TRANUSA recommended deploying it enterprise-wide instead: every user inside the CUI environment, with commercial Microsoft 365 kept out of CUI scope entirely.

On paper the narrow enclave is cheaper. In practice it hands the client a standing job — keeping controlled data inside a three-person boundary, keeping everyone else out of it, and being able to prove both. That work belongs to the business. Physical and logical access segregation is not something a security compliance MSSP performs on a client's behalf, and for a shop with no internal security director it is a burden that does not get sustained. The first spill undoes the compliance the partition was meant to protect. Scoping the enclave enterprise-wide cost more up front and removed that job entirely, along with the need to redraw the boundary every time the business changed shape.

The network was the hard part

It surfaced when the existing equipment could not be configured for the level of segmentation the framework requires — and the hardware was not FIPS 140-2 compliant, which no amount of configuration would have fixed. TRANUSA carried out a full network revamp: certified FIPS 140-2 hardware, and logical segmentation designed so the path controlled data takes through the environment is deliberate and documented. The client can now show an assessor exactly how CUI stays protected rather than describing it.

The cutover ran after hours and over weekends. The CNC and laser lines never went down during production.

The program itself

TRANUSA deployed its full security tool stack and built out the complete set of controls required for CMMC Level 2. Where requests had previously been informal, we stood up a service desk and a client portal, so staff can see what they submitted, what was said about it, and how it was resolved.

The division of labor is deliberate. Frontline day-to-day support stays with the client's own IT; TRANUSA sits behind it as Tier 2 and Tier 3 escalation. We are the client's security compliance MSSP, not their operational IT department, and the engagement was structured that way on purpose.

Application control was introduced the way it has to be in a production shop. The Zero Trust platform spends roughly thirty days learning what normal operation looks like before it moves into enforcement, so ordinary work is part of the baseline rather than a casualty of it. After that, system-level changes go through a whitelisting process. That friction is real, and it is a requirement of the framework rather than a preference of ours — the job is to sequence it so it never arrives on the shop floor unannounced.

03 The Outcome

The client reached a Supplier Performance Risk System score of **110 out of 110** and continues to win and retain Department of Defense work in a market where CMMC compliance has become a baseline requirement to compete at all.

Over the following year the shop roughly doubled in headcount without ever having to re-engineer its compliance boundary. That is the enterprise-wide enclave decision paying off directly: new people land inside a CUI environment that is already compliant, instead of triggering a scramble to widen an enclave every time the business grows.

04 Where Things Stand Today

The client is fully compliant and audit-ready at 110 out of 110 on SPRS, and has not yet been certified by a C3PAO. **These are different claims:** the compliance work is done and evidenced; the formal certification has not been issued.

The engagement is active and ongoing, and TRANUSA maintains the evidence locker continuously rather than assembling it ahead of a deadline. The remaining step is the assessment itself, not further remediation.

The client has also brought in several C3PAO assessors independently to run mock assessments against the environment. Each has responded positively to the deployment. That is informal feedback rather than a formal determination, but it is outside eyes on the work.

> THE DECISION THAT CARRIED IT
>
> A narrow enclave is cheaper on day one and hands the client a standing job. Scoping it enterprise-wide cost more up front and removed the job entirely — along with the need to redraw the boundary every time the business changed shape.

05 What We Learned

- **For small manufacturers, the hardest gap to close is usually physical.** Network equipment that has run a shop floor reliably for years is often incapable of the segmentation the framework requires, and consumer-grade hardware is not FIPS 140-2 compliant no matter how it is configured. It is the least visible line item in a compliance budget and frequently the largest, and most owners do not discover it until an assessment is already underway.

- **The standard path is not the only path.** Compliance for a DIB manufacturer is usually quoted as a migration to GCC High, and for many shops that is genuinely the right answer. For a small shop where the migration cost and the production disruption are prohibitive, a properly scoped enclave alongside the existing tenant can meet the same requirement without stopping the work that funds it. The right architecture depends on where the client actually is, not on which product the provider prefers to sell.
- **Scope decisions deserve to be challenged early.** This client planned to put three people in the CUI enclave — cheaper on day one and the obvious choice on a spreadsheet. Putting the whole organization inside it cost more up front and removed an entire category of future problem: no partition to police, and no re-scoping exercise every time someone new needs access to controlled data. Roughly doubling in headcount over the following year without a compliance bottleneck is the proof.

06 The Stack Behind It

Every engagement is backed by the same tool stack and operating model, regardless of client size. TRANUSA does not operate a staffed watch floor and does not describe itself as one.

- Continuous SIEM alerting with 24/7 escalation to TRANUSA on-call engineering
- Threat intelligence and log aggregation hosted on U.S. private cloud infrastructure
- Zero Trust endpoint defense with default-deny application control
- Continuous vulnerability management, prioritized by risk and CUI proximity
- SLA-driven patch management, with critical patches deployed to defined, reportable targets
- Enterprise GRC practice, including System Security Plan and POA&M management
- 100% U.S. Persons — no offshore personnel or subcontractors inside the compliance boundary

See what audit-ready looks like for a shop your size

Thirty-minute readiness call. calendly.com/tony-tranusa/cmmc-readiness-call · CMMC@tranusa.com

---

About this document. TRANUSA Case Study TUSA-CASE-002, version 1.0, issued 11 September 2026 by TRANUSA, LLC, Buford, Georgia. Public; may be forwarded freely.

Basis. TRANUSA engagement records, reviewed with the client before publication. Client identity, location and exact figures are withheld under the engagement agreement.

Limitations. This describes one engagement and is not a prediction of results for any other organization. TRANUSA is not a C3PAO and cannot issue a CMMC certification. “Compliant and audit-ready” and “certified by a C3PAO” are different claims and are distinguished in the text above. Current as of the issue date.