// WHAT SITS UNDERNEATH THE PROGRAM

CMMC-Categorized. GCC High Native.

Every component selected and categorized against CMMC Level 2 requirements, operated by U.S. Persons, and stopping at a hard line: our tooling processes telemetry only. Your controlled content never leaves your boundary.

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

01 The platform is the mechanism, not the product

What you are buying is a defensible compliance position: a boundary that holds, documentation that matches the environment, evidence with a history, and a score that survives examination. The platform underneath is how that gets operated. It matters, and it is not the point.

We say this plainly because the alternative is how most of this market is sold. A stack is a week of procurement and every provider can quote the same products. A program that survives an assessor, and keeps surviving one, is a different thing entirely.

02 What we operate

SIEM & alerting
U.S. private-cloud log aggregation with retention mapped to NIST SP 800-171.

Endpoint detection
Next-generation EDR on every in-scope endpoint.

Application control
Zero-trust allowlisting, run in learning mode before enforcement.

Patch management
Baselines and patching to defined, reportable targets.

Vulnerability management
Continuous scanning, tracked to closure.

GRC platform
SSP, POA&M and the evidence repository, kept current.

Identity & MFA
Sovereign identity, conditional access, enforced multi-factor.

Microsoft 365 GCC High
The U.S. sovereign Microsoft environment built for CUI and ITAR data.

WHAT WE DO NOT CLAIM

TRANUSA does not operate a staffed watch floor, and we will not describe it as one. What we run is continuous SIEM alerting with 24/7 escalation to TRANUSA on-call engineering, staffed by U.S. Persons. Some providers market that as a 24/7 SOC. We would rather you know exactly what you are buying, because an incident is the wrong moment to discover what a provider actually meant.

03 Where our boundary stops

Telemetry only. Never your controlled content.

TRANUSA tooling processes Telemetry Data only — logs, alerts and metadata. Your Controlled Unclassified Information and your ITAR-controlled technical data never leave your boundary and never enter ours.

This is architectural rather than a policy promise. It is written into our mutual NDA, it is a large part of why the arrangement is defensible under ITAR and EAR, and it is the first question a serious export-compliance officer should ask about any provider.

04 Asset categorization, applied properly

Most assessment trouble in a manufacturing environment comes from assets nobody categorized. We apply the CMMC categories across the whole environment, including the awkward ones.

Category	What sits here
CUI Assets	Workstations, servers and storage that touch Controlled Unclassified Information. Fully in scope, fully controlled.
Security Protection Assets	Our monitoring, logging, endpoint and GRC tooling. Categorized as SPA under CMMC guidance — which is what makes the arrangement assessable rather than a question mark.
Contractor Risk Managed Assets	Network equipment and peripherals that could touch CUI but are managed to reduce that risk, with the controls documented.
Specialized Assets	OT, CNC controllers, DNC boxes and shop-floor equipment — isolated and documented rather than pretended away. This is where generalist providers usually come unstuck.

05 We hold ourselves to the standard we set

TRANUSA brought its own environment into NIST SP 800-171 compliance, operates its own Microsoft 365 GCC High tenant, and runs its stack in U.S. sovereign cloud with a U.S. Persons-only team. Every control we ask a client to implement, we implemented on ourselves first.

TRANUSA is pursuing its own CMMC Level 2 certification. We are not publishing a target date, because the third-party assessment mechanism is currently suspended and a date we cannot control is not a commitment worth making in print. We will say so plainly when it is achieved.

- **Validated stack.** The same tools run our own operations. No client is the first deployment.
- **Real-world controls.** Implementations are tested in a live sovereign-cloud environment before client deployment.
- **Shared obligations.** We operate under DFARS 252.204-7012 and ITAR/EAR ourselves.
- **U.S. Persons only.** No offshore access to any client environment, at any tier, for any reason.

06 Where we sit in your support model

TRANUSA is not your IT department and does not replace it. Your frontline support stays yours; we sit behind it as Tier 2 and Tier 3 escalation for the compliance environment. That boundary keeps accountability clear and keeps us focused on the thing you are paying for.

See how the stack maps to your environment

Thirty-minute readiness call: we will walk the categories against what you actually run, including the shop floor.
calendly.com/tony-tranusa/cmmc-readiness-call · CMMC@tranusa.com

---

About this document. TRANUSA Capability Document TUSA-CAP-002, version 1.0, issued 11 September 2026 by TRANUSA, LLC, Buford, Georgia. Public; may be forwarded freely. Supersedes the earlier Security Stack technical brief, which carried a certification target date that is no longer published.

Basis. TRANUSA's deployed tool stack and internal compliance posture as of the issue date; CMMC asset categorization guidance; NIST SP 800-171 Rev. 2; and DFARS 252.204-7012.

Limitations. This document describes TRANUSA's approach and capabilities. It is not legal advice, not an assessment of any particular organization, and not a representation about any client's compliance status. TRANUSA is not a C3PAO and cannot issue a CMMC certification. CMMC program status is changing; verify any regulatory statement against the primary source before relying on it in a contract decision. Current as of the issue date above.