

Mission & Goal

CMTL, Inc. was formed on April 21, 2026, in Newport Beach, California. The company is currently operating as a “non-revenue producing public service organization”.

CMTL chose not to file to as a non-profit corporation to preserve the right to provide consulting services to enterprise memory module clients. This transition will potentially occur only if a compelling reason arises to facilitate a revenue generating business arrangement.

CMTL Primary Mission: Encourage and motivate enterprise server users and system integrators to implement procedures to secure their memory module procurement channels as soon as practical and possible to do so.

CMTL Primary Goal: Prevention and mitigation of advanced memory module fraud and potentially catastrophic security risks to enterprise servers and data centers. Fraud and security risks are currently being enabled by counterfeit, degraded, stolen memory components and modules with embedded malicious code.

CMTL Strongly Recommends: Enterprise memory module supply chain management implementation of processes to secure procurement channels including, but not limited to:

1. **Supplier Auditing:** Evaluate suppliers by auditing requirements to ensure adherence to strict quality controls and traceability standards.
2. **Product Auditing:** Conduct un-announced random sample audits of new incoming memory modules and modules currently deployed in the field.
3. **Fraud Mitigation:** Develop security frameworks to stop memory theft, "gray market" diversion, and tampering during shipping and warehousing.
4. **Counterfeit Detection:** Implement protocols to verify the authenticity of DRAM and flash memory chips, preventing altered or mislabeled parts from being used.
5. **Risk Management:** Diversify procurement to avoid relying on compromised or high-risk suppliers.

CMTL Industry Warning: Enterprise memory modules require specialized supply chain integrity services because a single counterfeit, degraded, tampered memory module or SSD can cause massive data center downtime, critical data corruption, and catastrophic security breaches.

CMTL Strongly Encourages: Memory component and module manufacturers, suppliers and customers to implement some form of blockchain technology. The type of blockchain distributed ledgers recommended for the computer memory industry is permissioned, consortium or hybrid.