Stephenson Stellar®
Corporation
Securing What Matters

Core Competencies

C1: Secure, Resilient Space and Terrestrial Communications - Assurance of mission-critical communications under cyber and kinetic stress. Covers secure communication link architectures, encryption, authentication, and anti-jam techniques, resilient cross-link and ground relay designs, and continuity of operations under cyber-attack, jamming, or partial constellation loss.

C2: Full-Spectrum Offensive and Defensive Cyber: Apply full-spectrum offensive and defensive cyber expertise to space, terrestrial, and cyber-physical systems to ensure mission resilience against advanced threat actors. Employ structured threat modeling methodologies (e.g., MITRE ATT&CK), mission-based cyber risk assessments, and kill chain mapping tailored to space and distributed architectures. Conduct vulnerability research, penetration testing, red-team and adversary emulation exercises across spacecraft, ground systems, transport networks, embedded systems, and mission applications. We assess attack surfaces spanning command and control pathways, supply chain dependencies, cryptographic implementations, identify infrastructure, and cross-domain interfaces.

C3: Secure Software Development & Mission Applications - Built-in security for mission-critical software systems. Covers secure DevSecOps pipelines for space, airborne, and ground software, supply chain risk management and software assurance, compliance with DoD, IC, and DHS cybersecurity standards without sacrificing agility.

C4: Data Science, AI/ML and Emerging Technologies - Advanced analytics to address scale, speed, and complexity of modern missions. Covers AI/ML-enabled data fusion across space, cyber, and terrestrial domains, on-board and edge analytics for warfighting platforms, explainable AI for operational trust and decision support, and advanced analytics for sensor fusion, targeting and tracking, anomaly detection, and system health monitoring.

C5: On-Orbit & Distributed Data Fusion - Architectures enabling timely, resilient decision-making. Includes trade studies comparing on-orbit versus airborne versus ground-based fusion, distributed processing across constellations, latency, bandwidth, and resilience optimization, integration with joint and coalition fusion environments.

C6: Critical Infrastructure Protection and Cyber Resilience - Application of mandated security principles to terrestrial infrastructure. Covers protection of power, water, transportation, emergency services, space-enabled backup communications and timing for infrastructure resilience, cross-domain dependency analysis between space services and infrastructure systems, cyber-physical risk modeling and resilience planning.

C7: Architecture Design: Design secure, resilient mission architectures across space, ground, transport, and hybrid environments. Integrate cybersecurity, mission assurance, and performance engineering at the system-of-systems level from concept development through operations. Our expertise spans secure spacecraft bus and payload integration, Zero Trust-enabled command and control, identity centric access control, protected communications pathways, distributed processing, and data fusion architectures. Conduct rigorous trade studies to optimize latency, bandwidth, SWaP constraints, and operational timelines, ensuring systems are engineered to perform reliably in contested, high consequence environments.

C8: Architecture Protection: Engineer layered, Defense-in-Depth protection strategies that safeguard mission systems against cyber, electronic, and supply chain threats. Embed Zero Trust principles, strong encryption and authentication, crypto agility, adversary informed threat modeling, and survivability engineering across spacecraft, transport networks, ground systems, and mission applications. Design architectures capable of detecting, isolating, and recovering from compromise while maintaining command integrity and continuity of operations, even in denied, degraded, intermittent, and limited (DDIL) conditions. Security is not an overlay; it is engineered into the foundation of every system we support.

C9: Architecture Validation: Provide independent architecture assessment and mission assurance to ensure systems are not only secure by design, but resilient in practice. Conduct objective trade analysis, risk-based security evaluations, adversary emulation, and performance assessments across space and cyber physical systems. Our validation efforts maximize real-world operational feasibility, resilience under advanced threat conditions, and the effectiveness of detection, response, and reconstitution mechanisms. By bridging engineering, cybersecurity, and operational perspectives, we deliver trusted insight that informs executive decisions and strengthens mission confidence.