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: Full-spectrum cyber expertise for space and distributed systems. Utilizes threat modeling, mission-based risk assessment, and kill-chain analysis. Includes vulnerability research, penetration testing, and adversary emulation. Covers spacecraft, ground systems, networks, supply chains, cryptography, 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.

Stephenson Stellar Corporation | 2031 Kings Highway, Shreveport, La 71103 | www.stephensonstellar.org

C7: Architecture Design: Provide secure, resilient mission architectures across space, ground, transport, and hybrid environments. Integrates cybersecurity, mission assurance, and performance engineering at the system-of-systems level. Includes Zero Trust command and control, identity-centric access, protected communications, distributed processing, data fusion, and optimized performance under constraints.

C8: Architecture Protection: Provide layered, defense-in-depth protection for mission systems against cyber, electronic, and supply chain threats. Incorporates Zero Trust, strong encryption, crypto agility, and survivability engineering. Ensures detection, isolation, recovery, and mission continuity, with security engineered as a foundational system element.

C9: Architecture Validation: Provide independent architecture assessment and mission assurance for secure, resilient systems. Includes trade analysis, risk-based evaluations, adversary emulation, and performance assessment. Validates operational feasibility, resilience under advanced threats, and effectiveness of detection, response, and recovery, informing decisions and strengthening mission confidence.