Executive Summary

This System Security Plan (SSP-Lite) documents the cybersecurity posture of the Frontier Field Services LLC Controlled Unclassified Information (CUI) Information System and provides a readiness baseline against the security requirements of **NIST Special Publication 800-171 Revision 3**. The purpose of this assessment is to identify the current implementation state of required safeguards, establish a defined CUI system boundary, and support organizational risk management and future compliance activities.

The Frontier Field Services CUI Information System is a hybrid environment composed of cloud-based collaboration services, on-premises file storage, managed endpoints, and managed mobile devices supporting operational field activities. Microsoft 365 is the primary platform for CUI collaboration and communication. The defined system boundary includes all systems that store, process, transmit, or administer access to CUI. Personal devices, unmanaged systems, and third-party environments outside Frontier Field Services' administrative control are explicitly excluded from the CUI boundary.

The assessment determined that Frontier Field Services has implemented a baseline set of administrative, technical, and physical safeguards designed to protect CUI. These include centralized identity and access management, use of managed devices, endpoint security protections, access restrictions based on defined roles, and facility-level physical access controls. Organizational roles and responsibilities for system ownership, security oversight, and technical administration have been identified.

The evaluation also identified areas where implementation maturity is incomplete or informal. Observed weaknesses primarily relate to governance, consistency, and documentation of security practices. Key improvement areas include mobile device security enforcement, audit logging coverage and review procedures, removable media governance, physical access documentation, maintenance procedures, and vulnerability tracking practices. These deficiencies are documented and tracked within the organization's Plan of Action and Milestones (POA&M).

This SSP-Lite does not assert full compliance with NIST SP 800-171 Revision 3. Instead, it provides a transparent representation of the current implementation state and establishes a structured foundation for remediation planning. The POA&M serves as the authoritative mechanism for managing corrective actions, prioritizing risk reduction efforts, and monitoring progress over time.

This document is intended to support internal risk management, leadership decision-making, and readiness preparation for future contractual or regulatory cybersecurity requirements. The protection of CUI is recognized as an ongoing operational responsibility requiring sustained governance, resource allocation, and continuous improvement.