UA-UA Strategic Coordination Service Description Document

General Service Description	
Service description identification	**Title:** UA-UA Strategic Coordination Service Description **Edition:** v1.1 **Reference Date:** June 13, 2024
Service identification	**Name:** ASTM F3548-21 Strategic Coordination Service
Service abstract	This ASTM F3548-21 standard-based strategic coordination service is aimed at mitigating the worst credible outcome of collision between two or more UAS per FAA Order 8040.6A.
Service Characteristics	
Service standard reference	**Service standard reference:** Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability (ASTM F3548-21) **Implemented options of the service standard:** ● Priority level for all operational intents will be set to 0 ● Conflicts are not permitted within the same priority level ● Per FAA NTAP requirements, Service Providers shall retain data received from other service providers for a minimum period of 45 days. ● Requirements in Section 2.4 regarding down USS not used
DSS configuration	DSS configuration process - as defined by InterUSS DSS Pooling
High-level Description of Service Offer	
Operational environment	Refer to ASTM F3548-21 Sections 4.2.4-4.2.7 for operational needs addressed by the service and the capabilities offered by the service.
Service functions	Refer to the following ASTM F3548-21 sections for functions offered by the service and their real world effects. ● Sections 10.4, 10.5, 10.6, 10.7, 10.11, 10.12
Limitations and Constraints on Using the Service	
Service access and use conditions	Refer to the applicable UAS Service Provider Data Sharing and Governance Agreement and Operator - Service Provider Agreement
Security and Privacy Aspects	

Security	Refer to ASTM F3548-21 Sections 5.2 and A2 for security requirements. Relevant requirements are listed below: * GEN0005 - USSs performing any of the roles identified in this specification shall be implemented and operated under an ISO/IEC 27001-compliant Information Security Management System or equivalent. * DSS0200 - DSSs shall authenticate with other DSS instances in the same pool using an industry-standard authentication mechanism. * DSS0205 - Communication between DSSs shall be encrypted using an industry-standard encryption mechanism with a minimum encryption strength of 128 bits. Service Provider may demonstrate equivalent compliance to ISO/IEC 27001 by providing a written attestation that the Service Provider materially complies with ISO/IEC 27001 or has implemented an Information Security Management System that includes the following: ● **Risk Assessment.** Annual information security risk assessment of UTM systems. ● **Access Control.** The Service Provider will limit access to its UTM Service and Shared Data solely to Service Provider employees and contractors who need access to perform their duties. The Service Provider has sufficient controls in place to prevent unauthorized access to its UTM Services and Shared Data. At a minimum such controls will include multi-factor authentication, periodic review of access privileges, and immediate revocation of access privileges upon an employee's termination. ● **Data Control.** Shared Data obtained in the operation of UTM Services is encrypted in transit. Shared Data is stored only on systems controlled by the Service Provider or via security-certified vendors. ● **Monitoring**. Systems used in providing the UTM Services are monitored for configuration drift and unauthorized access. All employee endpoints run malware screening and remediation tooling. ● **Incident Response**. Established process for incident response and breach notification.
Privacy	Refer to ASTM F3548-21 Sections 5.2 and A2 for security requirements. Relevant requirements are listed below: * USSs performing any of the roles identified in this specification shall (GEN0010) be implemented and operated under an ISO/IEC 27701-compliant Privacy Information Management System or equivalent. For initial production flights, Service Providers may demonstrate equivalent compliance for ISO/IEC 27701 as required by ASTM F3548-21 as follows: ● A Service Provider conforms with the terms set forth in Annex

	D (Data Privacy) ● A Service Provider completes an annual self-assessment and makes a written attestation during onboarding that the Service Provider materially complies or has implemented the following: ○ Conduct annual privacy risk assessment. ○ Implement privacy controls as part of a Privacy Information Management System (PIMS). ○ Implement privacy and security roles and responsibilities. ○ Define and adhere to a consent management process. ○ Manage Data Subject Rights (including as set forth in Annex D). ○ Establish processes for incident response and breach notification.
Authentication	Per ASTM F3548-21, Appendix X1 - Reference architecture for interoperability security controls, The X1.1 Base Deployment: Access Tokens with Audience Claims is implemented. Authentication and Authorization for communication between USS-USS and USS-DSS shall be facilitated by a common interoperability token exchanger service supporting OAuth 2.0. Auth provider should be ISO27001 certified or approved equivalent
Quality Aspects	
Quality of service	Refer to ASTM F3548-21 Section 5.2 for quality of service requirements. Relevant requirements are listed below: *GEN0015 - USSs performing any of the roles identified in this specification shall be implemented and operated under an ISO/IEC 9001-compliant Quality Management System, or equivalent. Service providers may demonstrate equivalent compliance to ISO/IEC 9001 by providing a written attestation that the Service Provider materially complies with ISO/IEC 9001 or has implemented a quality management system that includes the following: ● Quality policy ● Procedures to identify and document key processes and procedures for maintaining, testing, and updating the UTM Services ● Process for identifying, investigating, and addressing quality issues and implementing corrective and preventive actions ● Criteria for selecting and monitoring suppliers and subcontractors to ensure they meet quality requirements ● Plan for fostering continual improvement that includes employee feedback and initiatives to enhance effectiveness and efficiency of processes.
Service verification	Service will be verified using the InterUSS Automated Test Baseline

information	prior to SW deployment using test baseline identifier TB-c45a113 Verification test configuration to be defined by the Operations Committee
Safety	Service providers will conduct a hazard analysis to identify and mitigate safety risks in accordance with the process outlined by the GUTMA Safety Task Force Paper "USSP's Safety Support Assessment"
Performance Requirements	
Nominal service behavior	Refer to the attached Requirements Traceability Matrix, *Strategic Coordination V1.1 Compliance Matrix (ASTM F3548-21)*, for service performance and verification requirements
Degraded service behavior	For initial production flights, notifications regarding degraded service behavior will sent per the terms in the applicable UAS Service Provider Data Sharing and Governance Agreement and Operator-Service Provider agreement
Operational Intents	Operational intents ensure 95% conformance and are developed per the standard