UA-UA Strategic Coordination Service Description Document

General Service Description	
Service description identification	**Title:** UA-UA Strategic Coordination Service Description **Edition:** v1.4 **Reference Date:** Jun 5, 2025
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.
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 information	The Strategic Coordination Service including associated DSS interoperability will be verified prior to SW deployment using the following InterUSS Automated Test Baseline identifiers mapped to applicable Operations Committee test configurations or the Service

	Provider Gate 1 internal test environment: ● Gate 1 Service Provider internal test environment and pre-qual, early integration assessment, simulation fitness test configurations: TB-87bc766 ● production fitness test configuration which includes verification of system versions per ASTM F3548-21 requirement GEN0305: TB-59dff31
Discovery and Synchronization Service (DSS) configuration	DSS configuration process - as defined by InterUSS DSS Pooling instructions on joining an existing pool with new instance. **Requirements for confirming DSS pooling integrity** Upon joining a pool, USS shall verify the Dynamic Airspace Representation Identifier matches the published Dynamic Airspace Representation Identifier for the pool. The first instance of the DSS will provide the published Dynamic Airspace Representation Identifier for other pooling entities. USS shall continuously monitor that Dynamic Airspace Representation Identifier for their DSS instances match the DSS pool. Continuously is defined as at least once every 24 hours. For CockroachDB implementation, USS shall notify when pool health metrics are not in bounds within 1 minute of occurrence. In bound health metrics include: ● Unavailable Range = 0 Under nominal operating conditions, unavailability is indicative of cluster misconfiguration. ● SQL Failure Count = 0 SQL Failure count is a rare but serious indication of a malformed query. Alerting on it in earlier environments helps ensure that an incorrect DSS version update never reaches production. ● Active node metric absence for a rolling 5 minutes window. Metric absence indicates that the state of the cluster is unknown and indicates an inability to monitor critical metrics of the system. ● Node restarts <= 1 within an hour. Frequent restarts indicate instability.
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 V1.2 Compliance Matrix (ASTM F3548-21)*, for service performance and verification requirements
Degraded service behavior	Notifications regarding degraded service behavior including DSS degradation will be sent per the terms in the applicable UAS Service Provider Data Sharing and Governance Agreement and Operator-Service Provider agreement. Mitigation of a Severity 1 issue as defined in the applicable UAS Service Provider Data Sharing and Governance Agreement includes a service provider marking their own availability state as down in the DSS until the issue is resolved. DSS-related service degradation detected per the requirements for confirming pooling integrity and provision of DSS instances are Severity 1 events.
Operational Intents	Operational intents ensure 95% conformance and are developed per the standard
DSS pool	To participate in the deployment of a DSS pool, a USP must meet the following minimum infrastructure requirements: **Configuration** ○ Provide exactly 3 CockroachDB nodes ○ Each node must have at least ■ DNS resolution or stable public static IP to enable node discovery ■ Port 26257 availability for inter-node communication ■ DSS core service version v0.20.0 ■ CockroachDB version v24.1.3 **Provision of DSS instances** These requirements ensure effective minimal provision of DSS instances. It is also recommended that Service Providers adhere to InterUSS recommended sizing and proactively monitor conditions at lower levels to reduce the likelihood of exceeding these requirements. ○ USS shall provision DSS instances with the necessary resources to maintain CPU usage of < 90%. ○ USS shall notify if CPU usage >=90% for more than 1 consecutive hour. ○ USS shall provision DSS instances with the necessary resources to maintain memory usage of < 90%. ○ USS shall notify if memory usage >=90% for more than 1 consecutive hour.

- USS shall provision DSS instances with the necessary resources to maintain IOPS in progress < 10.
- USS shall notify if IOPS in progress >=10 for more than 5 consecutive minutes.
- USS shall provision DSS instances with the necessary resources to maintain <=100ms P50 Round Trip Time (RTT) between DSS instances. 100ms is based on the nominal performance for inter cloud RTT times within the continental US as an initial target value.
- USS shall notify if P50 Round Trip Time (RTT) > 100ms more than 5 consecutive minutes.
- For CRDB implementations, the following definitions apply

Requirement	**CRDB metric per CRDB node**
CPU Usage	sys.cpu.combined.percent-normalized
Memory	sys.rss
IOPS in progress	sys.host.disk.iopsinprogress
Storage	capacity.used
P50 Round Trip Time (RTT)	round-trip-latency (50 Percentile)

As of the reference date of this SDD, the following configuration generally meets the above Provision of DSS instances requirements

- CPU: At least 4 cores; 8+ cores recommended, with support for virtualization and containerization.
- RAM: At least 8GB of memory; 16GB+ recommended.
- Storage: SSD-based storage with at least 100GB available per node (expandable based on dataset size and replication needs).
  - Minimum IO/s 3000 R/W
  - Minimum throughput 125 MB/s R/W
  - Maximum average latency 5ms R/W
  - Maximum P99 R/W latency 10ms
- Network: High-speed (10+Gbps) low-latency network with a stable public IP address
- Accurate system time using NTP synchronization from Google's Public NTP source