JTAC Mission Support

SPONSORING ORGANIZATION

Aeronix Corporation

CHALLENGE

Drones from Small Unmanned Aircraft Systems (SUAS) to long-endurance loitering munitions are increasingly pivotal to sensing-to-shooter loops, but they remain only partially and unevenly integrated into theater Command and Control (C2) and Joint All-Domain Command and Control (JADC2)-style architectures because tactical networks, coalition enclaves, and high-classification sources are separated by policy, accreditation, and technical guards that impede timely, auditable data flows. Key literature identifies five recurring friction points: cross-domain transfer, provenance/labeling, accreditation & policy, contested Electromagnetic Spectrum / Electronic Warfare (EMS/EW) environments, and resource/edge limitations (compute, Size, Weight and Power (SWaP), latency).

This challenges military qualified service members who direct the action of military aircraft engaged in close air support and other offensive air operations from a forward position (Joint Terminal Attack Controllers or JTACs) who need rapid, authenticated targeting feeds with full provenance. Additionally, Rules of Engagement (ROE) / Legal Advisors need traceable, auditable trails of sensor-to-shooter data for post-strike review.

RELEVANT CONTEXT

- Modern doctrine (JADC2/CJADC2) aims to push sensing-to-shooter loops toward the tactical edge; this increases reliance on unmanned air systems (from small SUAS to long-endurance loitering munitions) as persistent sensors and effectors. For true integration, drones must participate in automated or semi-automated data flows (sensor → fusion → targeting → authorization → shooter) rather than remain isolated point assets.
- Current integration is uneven and largely experimental: service and joint demonstrations reduce latency in controlled events but stop short of fielding accredited, production patterns for passing classified, policy-sensitive data to edge weapons. In many theaters drones still operate in tactical stovepipes, disconnected from higher-classification fusion and decision authorities.
- The single largest practical friction is cross-domain transfers: classified/intelligence sources, service enclaves, and coalition networks are separated by policy and accreditation boundaries. Existing Cross-Domain Solutions (CDS) and high-assurance guards were designed for enterprise/classified enterprise use and are

often too heavyweight, too slow to accredit, or too resource-intensive (SWaP/throughput/latency) for tactical, low-SWaP drone gateways. Ruggedized and tactical CDS variants exist but remain limited in throughput, latency guarantees, and policy expressiveness.

- Provenance & labeling are critical. Targeting and sensor data must carry machine-readable provenance (source, confidence/quality, timestamp, sensor geometry), release authorities, and caveats so downstream operators or automated policy engines can make lawful, auditable release/engagement decisions. Lack of canonical schemas and inconsistent metadata labels prevents deterministic filtering and automated release decisions.
- Contested EMS/EW complicates integration. Jamming, spoofing, and spectrum congestion force routing and protocol tradeoffs that interact poorly with CDS expectations (which often assume robust links). Any tactical CDS pattern must be tested for degraded communications, failover routing, and graceful metadata degradation.
- Coalition & legal/policy constraints add another layer: selective sharing, bilateral caveats, and multilateral agreements require release rules more nuanced than simple classification gates. Solutions must enforce caveats and produce auditable trails suitable for legal/ROE review.
- Human workarounds are commonplace when automated, policy-aware cross-domain flows are unavailable: manual relay, chat-based coordination, pre-approved corridors, or human-mediated retransmission. These workarounds increase latency, cognitive load, and operational risk—especially under high tempo.

IMPACT

Increased decision latency (missed time-sensitive targets), higher fratricide and collateral risk from incomplete provenance/authorization metadata, and lost opportunities for decentralized, mission-tailored weapons employment. Proliferation of point-to-point gateways and bespoke translation layers increases integration cost, extends fielding timelines, and produces brittle, hard-to-accredit stacks for coalition use. Inability to safely and rapidly share classified or controlled data with coalition partners degrades deterrence and multi-domain campaigning. Evidence and oversight reports note these exact risks for CJADC2/JADC2 implementation.

BENEFICIARIES

- JTACs and forward controllers who need rapid, authenticated targeting feeds with full provenance.

- ROE/Legal advisors who need traceable, auditable trails of sensor-to-shooter data for post-strike review.

TEAM RECOMMENDED SKILLSETS

Computer Science, Cybersecurity, Data Science, Information Systems, Software Engineering, International Relations, Computer Engineering

PROBLEM SPONSOR

Mr. Tyler Jandreau, Director of Technology and Innovation
Aeronix Corporation