WHITE PAPER

REVRD: REAL-TIME EMERGENCY VEHICLE ROUTE DISPLAY

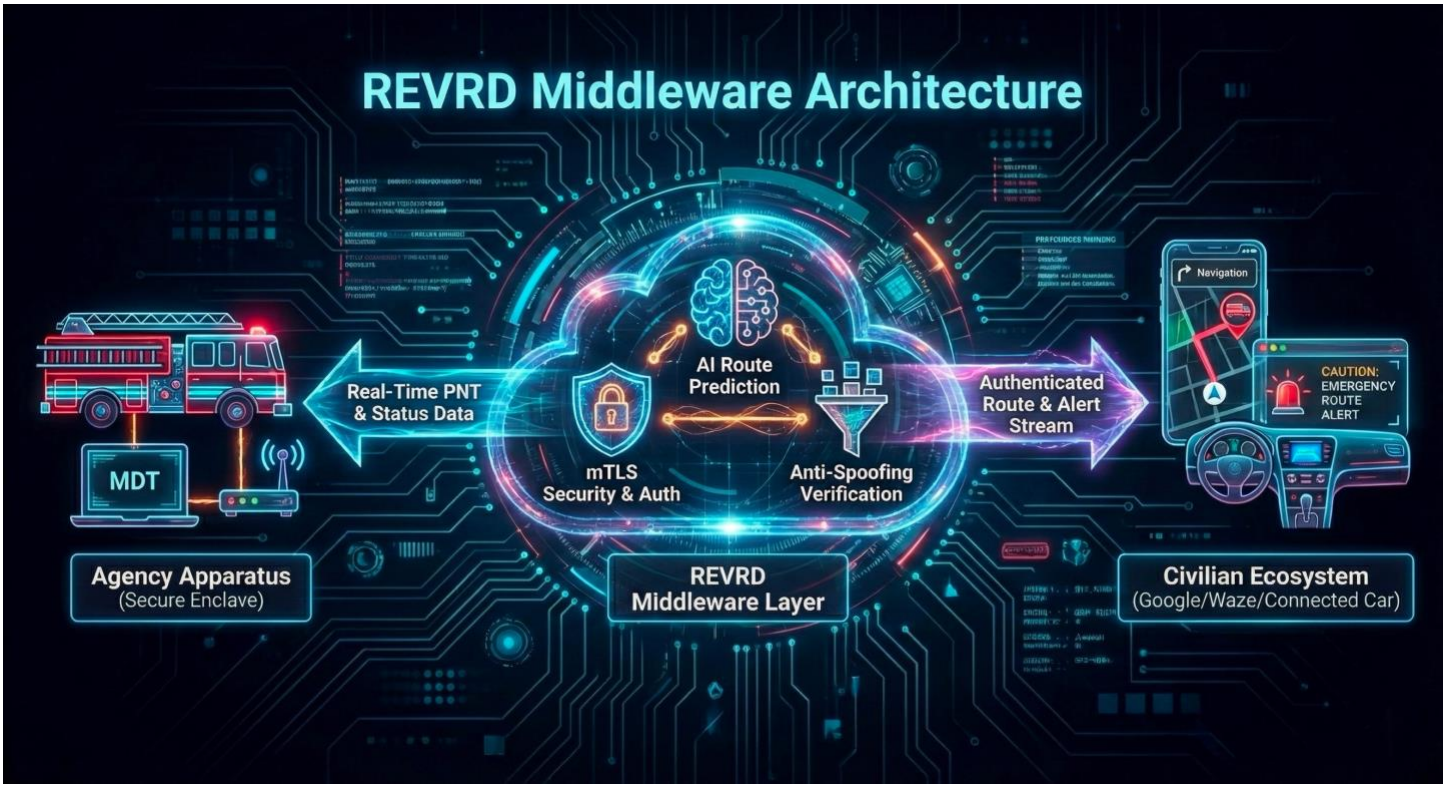
Date: December 24, 2025

By: REVRDTECH LLC

1. Executive Summary

REVRD (Real-Time Emergency Vehicle Route Display) is a patent-pending solution designed to bridge the gap between Fire/EMS apparatus and the civilian driver. Acting as a secure digital layer, REVRD ingests real-time Position, Navigation, and Timing (PNT) data from existing apparatus telematics and processes it to influence driver behavior and clear routes.

This document outlines REVRDTECH's adherence to the CISA "Secure by Design" principles. As a middleware provider, our security architecture focuses on the integrity of the data "bridge"—ensuring that the signal sent by the Fire Department is authenticated, secured, and delivered instantly to digital mapping platforms without latency or manipulation.



2. Middleware Architecture: The Secure Bridge

REVRD does not require proprietary hardware installation. Instead, it functions as an interoperable software layer (API) that connects distinct ecosystems.

2.1 Hardware Agnostic Integration

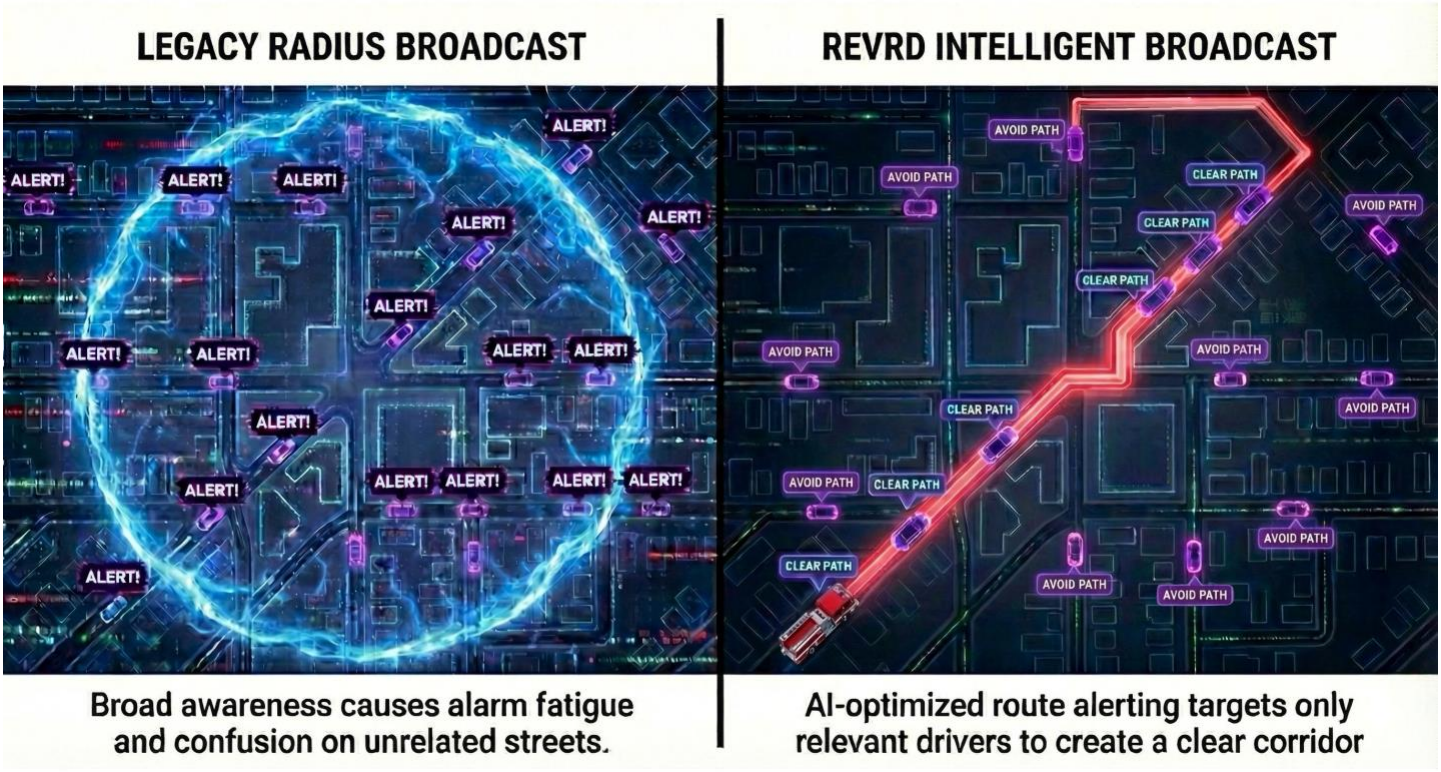
- The Bridge: REVRD integrates directly with existing Mobile Data Terminals (MDTs), CAD (Computer Aided Dispatch), and vehicle modems (e.g., Cradlepoint, Sierra Wireless) used by Fire Departments.
- Security Implication: Because we act as a bridge, we do not introduce new hardware attack surfaces. We leverage the existing secure enclave of the apparatus and apply a secondary layer of encryption to the data stream as it leaves the vehicle.

2.2 Secure API Gateway

- Authentication: We utilize mutual TLS (mTLS) authentication. The "bridge" only opens for verified agency endpoints. A spoofed signal attempting to enter the REVRD middleware layer is rejected immediately because it lacks the agency-specific cryptographic signature.
- Data Integrity: The data flowing across the REVRD bridge is immutable. We use cryptographic hashing to ensure that the location and status (e.g., "Lights and Sirens ON") cannot be altered by a man-in-the-middle attack between the fire truck and the cloud.

3. Context-Aware Alerting & Route Projection
REVRD utilizes Artificial Intelligence to optimize the accuracy and distribution of emergency data across the bridge.

3.1 Intelligent Route Visualization
- The Problem: Legacy alerting systems rely on static broadcast radii that lack geospatial context. They alert drivers that an emergency vehicle is nearby, but fail to indicate where it is coming from or where it is going.
- The Middleware Solution: REVRD's middleware ingests the active route from the fire apparatus and projects it directly onto public navigation systems.
- Operational Impact: By casting a dynamic awareness radius and visualizing the specific path of travel, REVRD creates a "corridor of clearance." This allows civilian drivers to anticipate the apparatus's movement and proactively yield the right-of-way before the physical siren is even heard.



3.2 Secure AI Execution
- Security: The algorithms responsible for processing this route data run in a sandboxed environment within the middleware stack. This ensures that any external data anomalies cannot feed back into or corrupt the Fire Department's critical dispatch systems.

4. PNT Resilience & Anti-Spoofing

As the middleware responsible for transporting location data, REVRD validates the payload before passing it on.

- Ingest Validation: REVRD acts as a filter. When PNT data enters our bridge from the apparatus, our algorithms cross-reference it with network telemetry. If the GPS data shows signs of spoofing (e.g., coordinates inconsistent with fire truck physics), the middleware flags the packet and blocks it from reaching civilian drivers to prevent confusion.
- Latency Management: As a real-time bridge, our architecture is optimized for sub-second latency (<100ms), ensuring that the "digital siren" matches the physical location of the truck.

5. Compliance & Data Sovereignty

REVRD respects that it is a processor of data, not the owner.

- Pass-Through Privacy: REVRD operates on a "privacy-by-design" basis. We bridge the alert data to the public to clear the road, but we do not retain or harvest surveillance data on civilian drivers.
- Agency Control: The Fire Department retains full sovereignty over their data. The REVRD bridge can be severed instantly by the agency (the "Kill Switch") if they wish to go dark for operational security, giving the Fire Chief ultimate control.

6. Conclusion

REVRDTECH provides the essential digital infrastructure to modernize Fire Service response without the burden of new hardware. By securing the data bridge between the apparatus and the connected world, we allow Fire Departments to leverage the power of AI and digital alerting while maintaining strict compliance with CISA and NIST security standards.