Digital Corridor Initiative (DCI)

Data Governance & Interoperability Working Group

Meeting Summary

October 29, 2026

Purpose and Context

The DCI Coalition Data Governance and Interoperability Working Group convened on October 29 to explore the governance, trust, ownership, and interoperability considerations necessary to support the sharing of data across jurisdictions and sectors. The session focused on work zone and lane closure data as a representative use case while recognizing that the governance and interoperability principles developed through this effort may apply to a broader transportation data ecosystem.

This working group was established specifically to examine how organizations can exchange transportation data across jurisdictions, agencies, and technology platforms while maintaining a baseline of trust, provenance, security, and accountability through the data lifecycle. Discussions were intended to complement parallel efforts in the Coalition's Data Collection, Quality and Validation working group by developing a practical farmwork for data governance and interoperability by April 2027.

Key Themes and Strategic Takeaways

1. **Trust requires visibility into Data Quality and Provenance.** Participants consistently identified that source attribution, validation status, update timing, and accuracy indicators are essential trust signals. Participants emphasized that trust is not established solely through adherence to standards, but rather through visibility into how data is originated, validated, updated, and modified through its lifecycle.

2. **Ownership must define rights, responsibilities, and stewardship.** Participants viewed data ownership as more than legal possession; it extends to publication rights, modifications, and permissions governing downstream use. Multiple participants noted that ownership and stewardship responsibilities must remain clear even as data moves between agencies, vendors, and service providers.

3. **Security should be risk-based.** Provenance, validation, and security requirements should not be fixed, but scaled according to the sensitivity and intended use of data. Participants recognized that real-time operational information and safety-critical applications may require different levels of oversight and protection. This suggests future governance frameworks should establish common baseline requirements while providing context-specific controls.

4. **Accountability must extend across the full data lifecycle.** Participants emphasized that accountability is shared, and should span data collection, processing, publication, aggregation, distribution, and operational use. Several participants highlighted the need for correction mechanisms that include independent verification processes in the event that failures occur within the broader data ecosystem.

5 **Participants shared consensus on a blended governance model.** Live polling results suggested that participants envisioned a governance framework that distributes responsibility across sectors rather than concentrating it in one organization or sector.

Attendance Snapshot

The session convened approximately 140 participants representing state departments of transportation, federal agencies, metropolitan planning organizations, transportation technology providers, operators, consultants, nonprofit organizations, and academic institutions. This diversity reflects the broad stakeholder ecosystem required to support a trusted transportation data exchange.

Category	Organizations in Attendance
State/Local Government	City of Peachtree Corners, Florida DOT, Georgia DOT, Maricopa Association of Governments, Michigan DOT, Nashville Department of Transportation & Multimodal Infrastructure, Oklahoma DOT, Texas DOT, Washington State DOT
Transportation Technology Providers	Cisco, Causeway Technologies Inc, Ersi, Ersi Canada, FlowLabs, Information Logistics, Inc. JMT Technology Group, Kapsch TrafficCom, Miovision, Mobilis Traffic, OmniTrust, P3Mobility, Pedestrian Safety Solutions, Valerann
Academic and Research Institutions	Carnegie Mellon University, Florida A&M University, Florida International University, Georgia Institute of Technology, Hellenic Institute of Transport, Howard University, Oklahoma State University, Texas A&M Transportation Institute, The Ohio State University, UC Berkely PATH, University of California Riverside, University of Houston, University of Louisville, University of Oklahoma, University of Texas at Arlington, University of Texas at Austin, University of Washington
Consultants, Engineering, Telecommunications	AECOM, Accenture, AEM Corporation, Arcadis, AtkinsRealis, Cambridge Consultants, Deloitte, HDR, HNTB, Iteris, Kimley-Horn, RS&H, STV, Tirhydro, Verizon, VHB, WSP
Nonprofit/Association	NOCoE / AASHTO, PrePass Safety Alliance, Smart Infrastructure Solutions, The Eastern Transportation Coalition

Opening Remarks and Context

The meeting opened with remarks from Tim Drake of Miovision, who provided framing for the discussion around a series of foundational data governance questions: What conditions are necessary for organizations to trust shared transportation data? How should ownership and accountability be managed? What security protections are required? And how can interoperability be achieved while

preserving organizational responsibilities and public confidence?

Immediately following, Morgan Fincher of ITS America provided an overview of the DCI Coalition, highlighting the mission to identify barriers and produce solutions to encourage the deployment of transportation digital infrastructure. Participants reviewed the relationship between the two working groups within the coalition, emphasizing that both workstreams are interwoven and necessary to enable a trusted and scalable transportation data exchange.

The group also reviewed working definitions for work zone data and the concept of a Shared Data Layer (SDL), which serves as a framework to enable a trusted exchange of data among multiple participating organizations while preserving ownership, accountability and transparency. The group was informed that further information on the SDL concept would be presented in ITS America's upcoming Shared Data Layer White Paper, slated for publication in December 2026.

Breakout Group Discussion Summary

Participants were divided into three facilitated breakout groups to examine four interconnected governance topics: trust, provenance, security, and accountability. Using Mentimeter to structure discussion, participants explored what information, controls, and institutional arrangements would be necessary for organizations to exchange transportation data across jurisdictions and organizational boundaries with confidence.

Across all breakout discussions, participants repeatedly identified data quality, validation, timeliness, provenance, ownership clarity, and accountability as foundational requirements for trust. Discussions highlighted a broad consensus that governance responsibilities extend beyond original data creators and should encompass all participants involved in collecting, managing, distributing and consuming transportation information.

Key Breakout Group Takeaways

Public Agencies Are Expected to Lead Governance. Polling results revealed a clear preference for public-sector leadership across most governance functions. State Governments received the strongest support for establishing trust (50%) and enforcing governance protocols (66%), while federal agencies received the strongest support for establishing ownership protections (62%) and security standards (78%). These results support a shared governance model that combines federal policy leadership with state-level implementation and oversight.

Provenance is Foundational to Trust. Participants consistently identified provenance as one of the most important requirements for a trusted data exchange. This includes source attribution, validation records, update history, and change tracking, which participants cited as necessary mechanisms for helping users evaluate data quality and reliability.

Security Should be Tiered and Context-Sensitive. Rather than uniform security standards across all transportation data, participants indicated a preference for a tiered approach to security that would scale protections to match both sensitivity and the potential consequences of misuse.

Accountability Must Follow the Data. Participants repeatedly emphasized that accountability should not end when data leaves the organization that created it. Governance frameworks should establish clear responsibilities throughout the data lifecycle and provide mechanisms for correcting errors, resolving disputes, and monitoring performance. Participants proposed the creation of an independent, coalition-governed third party responsible for ensuring accountability across the data lifecycle.

Shared Data Exchange Requires Clear Operating Rules. Ownership, usage permissions, publication authorities, and correction procedures have all emerged as fundamental requirements for transportation data exchange. Participants stressed that to trust data, common expectations must be defined regarding how data is contributed, modified, distributed, and consumed.

Path to April 2027

The October workshop established an initial governance foundation for the Coalition's broader digital infrastructure initiative. Findings from the session will be used to further define governance requirements, institutional responsibilities, and operational expectations to create a trusted transportation data exchange.

Over the coming months in future working group sessions, the coalition will continue to refine key governing concepts, including trust indicators, ownership protections, provenance requirements, accountability models, and security baselines. Future discussions will focus on translating these principles into a practical framework that can support interoperable data sharing across jurisdictions and sectors.

The results of this work will directly inform the development of a scalable framework for transportation digital infrastructure as it relates to work zone and lane closure data by April 2027.