ODOT/METRO

MULTIMODAL INTEGRATED CORRIDOR MANAGEMENT ARCHITECTURE

PACKET OF FINAL MATERIALS

DKS

720 SW WASHINGTON STREET, SUITE 500, PORTLAND, OR 97205 • 503.243.3500 • DKSASSOCIATES.COM

CONTENTS

SECTION 1. DATA SHARING NEEDS INVENTORY

SECTION 2. ITS ARCHITECTURE UPDATES

SECTION 3: DATA SHARING POLICY LANGAUGE

SECTION 1. DATA SHARING NEEDS INVENTORY

TECHNICAL MEMORANDUM, UPDATED JUNE 2021

DKS 720 SW WASHINGTON STREET, SUITE 500, PORTLAND, OR 97205 • 503.243.3500 • DKSASSOCIATES.COM

DATA SHARING NEEDS INVENTORY

DATE: June 2021

TO: Scott Turnoy | ODOT
Caleb Winter | Metro

FROM: Jim Peters, Dennis Mitchell, Kelly White | DKS Associates

SUBJECT: Multimodal Data Sharing Needs Inventory for Integrated Corridor Management

Project #20139-002

INTRODUCTION

In 2018, Metro and ODOT produced a pilot study report on integrated corridor management (ICM) on the I-84 corridor travel shed in Portland, Oregon. One recommendation from the study was to "Create a Data-Sharing Policy" to establish a common language to improve transportation-related data sharing capabilities across the region. The policy intends to provide an open data platform that improves information flow and availability to agencies, transportation system operators, and travelers. Access to multimodal data is foundational for operating the transportation network as efficiently as possible, both in real-time and when assessing past performance.

This technical memorandum identifies data sharing needs based on stakeholder input and a review of the current state of transportation data relevant for integrated corridor management in the Portland-Vancouver metropolitan area. The following sections describe:

- The stakeholder outreach process
- A high-level summary of current data availability
- Data gaps (including agency-identified data issues and concerns)
- High-level recommendations for data formats

A tabular version of the information described in this memorandum is included in the Appendix.

STAKEHOLDER OUTREACH PROCESS

The project team conducted outreach to stakeholders in the Portland-Vancouver Metropolitan area to gain insight on data needs for ICM. Table 1 indicates which agencies provided input. Outreach

consisted of two primary efforts: a core stakeholder group workshop and a general stakeholder group survey.

TABLE 1: AGENCIES PROVIDING INPUT

CLACKAMAS COUNTY	ODOT	SOUTHWEST REGIONAL TRANSPORTATION COUNCIL
C-TRAN	PORTLAND BUREAU OF TRANSPORTATION	TRIMET
FHWA	PORT OF PORTLAND	WASHINGTON COUNTY
METRO	PORTLAND STATE UNIVERSITY	CITY OF WILSONVILLE

CORE STAKEHOLDER GROUP WORKSHOP

On December 16th, 2020, the project team facilitated a virtual workshop for core stakeholders in the ICM data sharing space. Attendees included public agency stakeholders involved in the I-84 corridor ICM study in 2018 and those currently sharing and using data for ICM purposes. Key discussion points at the workshop included:

- Reviewed the data streams currently available, including operational assumptions and potential new data sources
- Visioning for successful data sharing, including what issues to address, what barriers currently exist, and brainstorming of what agreements could facilitate data sharing

A summary of the meeting is included in the Appendix, with a complete list of attendees.

GENERAL STAKEHOLDER GROUP SURVEY

The project team developed a survey with specific questions related to data availability, data sharing, and partnerships to reach a wider regional audience. Stakeholders included in the survey distribution were selected based on their expected involvement in ICM, despite whether they currently collect and share data or not.

The general framework of the survey was intended to:

- Frame the conversation with questions about how a respondent would use data for ICM
- Determine what data is already being collected for various modes and how that data is shared
- Prompt respondents to think about what data they could use to manage a corridor effectively
- Discover what concerns respondents have with respect to data sharing, including the relationship with third-party data providers and consumers

A copy of the survey and the list of respondents is included in the Appendix.

The following sections provide summaries of the feedback received through the outreach process via the workshop and survey.

CURRENT DATA AVAILABILITY

The project team determined the data types currently used for operations and traveler information through survey responses and research. Table 2 summarizes the data types that are available. The Appendix includes more information, including the agencies that collect each data type listed below.

TABLE 2. SUMMARY OF DATA TYPES CURRENTLY AVAILABLE

MODE	DATA TYPE
VEHICLE DATA	Volume, Speed, Travel Time, Incident Information, Vehicle Classification, Intersection Delay (Through Movement), ATSPMs
TRANSIT DATA	Volume, Ridership, Speed, Travel Time, Incident Information, Park and Ride Utilization, On-Time Performance, Bus on Shoulder Use, Transit Signal Priority (TSP) Calls
FREIGHT DATA	Volume, Incident Information, Vehicle Length
BICYCLE AND PEDESTRIAN DATA	Bicycle Volume, Pedestrian Volume, Trail Counts
TOWING DATA	Quantity of Tows, Response Times, Locations, Reason for Tow, Day and Time
OTHER DATA	Weather Information, Equipment Failure, Road Hazards, Video

IDENTIFICATION OF DATA GAPS

In addition to the data currently available for ICM, stakeholders were asked to share any data gaps. Table 3 provides a simple list of the identified data gaps. The Appendix includes additional information.

TABLE 3. STAKEHOLDER IDENTIFIED DATA GAPS

DEMOGRAPHICS FOR USERS OF DIFFERENT MODES	TRANSIT PERFORMANCE MEASURES
REAL-TIME METERED ON-RAMP USE	WIDESPREAD MULTIMODAL TRAVEL BEHAVIOR
EXPECTED BRIDGE LIFT TIME	SPEED BASED REAL-TIME BUS ON SHOULDER USE CONDITIONS
ROBUST MULTIMODAL PERFORMANCE MEASURES	

In addition to the data gaps listed above, two additional gaps in data usage/storage were identified by stakeholders:

- The lack of a regional, integrated data warehouse to store the region's data in one place
- The data, technical training and tools to provide operators with situational awareness

AGENCY-IDENTIFIED DATA ISSUES AND CONCERNS

In addition to data gaps, stakeholders identified several issues and concerns related to technical data issues and data sharing. Table 4 and Table 5 summarize the issues and concerns. The Appendix includes additional information.

TABLE 4. AGENCY-IDENTIFIED *TECHNICAL* DATA ISSUES AND CONCERNS

GENERAL THEME	CONCERNS
	TECHNICAL DATA ISSUES
STORAGE	Where should data be stored? Should the data be published in real-time? What resolution should data be? Where does data get archived?
SOFTWARE CAPABILITY	Will data be suitable for agencies to manage traffic actively?
COMMUNICATIONS INFRASTRUCTURE	Not every agency is connected to high-speed communications. At what level should there be communications (peer-to-peer intersection level)?
ADDITIONAL DATA TYPES	How to measure total person capacity for a corridor (including all modes)? How do we address gaps in multimodal data?
STAFF TIME	How do already time-constrained staff ingest and analyze other data effectively?

TABLE 5. AGENCY-IDENTIFIED *DATA SHARING* ISSUES AND CONCERNS

GENERAL THEME	CONCERNS
	DATA SHARING ISSUES
LIABILITY	Gatekeeper role of agency staff What level of control do agencies have over each other, especially during a significant event? How liable is each agency making decisions using data?
COMMON STANDARDS	What is the process when modifications to data sources are made?
PRIVACY	How to create unique identifiers for each agency and its data sources?
PRIVATE SECTOR INTEGRATION	How to see a regionally complete picture when some data is monetized? How to make sure private companies are committed to agency goals that benefit the public?
LAWS AND REGULATIONS	How do agencies meet the requirements of varying laws?
OWNERSHIP	Ongoing maintenance and upkeep Who is responsible for fixing a problem when it arises? Who is the regional owner? Who are the individual agencies responsible?

HIGH-LEVEL RECOMMENDATIONS FOR DATA FORMATS

Transportation data relevant for integrated corridor management is currently shared in a variety of formats, frequencies, and quality. There are several existing locations where the data described in Table 2 is being shared, including PSU's Portal Archived Database, ODOT's TripCheck API, and directly between agencies. At this point in the development of a formalized integrated corridor management process, a plan for a specific data format for each data source would be too prescriptive, especially given the fast-paced and everchanging nature of data sharing capabilities among agencies.

The following set of high-level recommendations are intended to inform the Data Sharing Policy that will shape Integrated Corridor Management practices in the Portland Metro region and throughout the state of Oregon. Each of the following bullet points describe essential elements of data that will be shared:

- Real-time
- Continuous[1]
- Appropriate detail and granularity to support decision making
- Commitment to quality from all sources, public and private
- Consistent standards/formats across agencies involved in data sharing

[1] Continuous data in the integrated corridor management context is information constantly being collected at an agreed upon time interval for operators to access.

SECTION 2. ITS ARCHITECTURE UPDATES

TECHNICAL MEMORANDUM, UPDATED APRIL 2021

DKS 720 SW WASHINGTON STREET, SUITE 500, PORTLAND, OR 97205 • 503.243.3500 • DKSASSOCIATES.COM

ITS ARCHITECTURE REVIEW

DATE: April 2021

TO: Scott Turnoy | ODOT
Caleb Winter | Metro

FROM: Jim Peters, Dennis Mitchell, Elliot Hubbard, Kelly White | DKS Associates

SUBJECT: ITS Architecture Review
for Integrated Corridor Management

Project #20139-002

INTRODUCTION

This memorandum presents recommended ITS architecture updates to support Integrated Corridor Management and a Multimodal Data Sharing Policy. It includes cybersecurity recommendations to support the data sharing elements identified in the previous memorandum (Task 2 – Data Sharing Element Needs Inventory).

PROPOSED ITS ARCHITECTURE UPDATES

The project team reviewed the TransPort Regional ITS Architecture to identify any changes needed to support the Integrated Corridor Management process's data sharing elements. The following section describes:

- Recommended ITS Architecture Service Package Updates
- A conceptual real-time data sharing architecture diagram

RECOMMENDED SERVICE PACKAGE UPDATES

Table 1 summarizes the nine ITS Architecture service packages that should be added or modified to support Integrated Corridor Management. Other service packages may be impacted or influenced by Integrated Corridor Management, but significant changes are not recommended at this time. The packages listed in the leftmost column of the table are reflective of the most recent version of the National ITS Reference Architecture (ARC-IT Version 9.0).

TABLE 1: RECOMMENDED SERVICE PACKAGE UPDATES

ARCT-IT 9.0 SERVICE PACKAGE		STATUS IN CURRENT ARCHITECTURE	CURRENT ARCHITECTURE ALIAS	EXPECTED IMPACT
CVO09	Freight-Specific Dynamic Travel Planning	Existing/Planned	-	Acknowledge the connection to freight through the ICM concept
MC06	Work Zone Management	Existing/Programmed	MC08	Acknowledge the connection to the ICM concept
MC08	Maintenance and Construction Activity Coordination	Future	MC10	Add to architecture with connection to ICM concept
PM02	Smart Park and Ride System	Future	ATMS17	Add to architecture with connection to ICM concept
ST06	HOV/HOT Lane Management	Future	ATMS05	Add to architecture with connection to ICM concept
TM09	Integrated Decision Support and Demand Management	Future	ATMS09	Add the institutional, operational, and technical integration
TM11	Road Usage Charging	Planned	ATMS25	Acknowledge the connection to the ICM concept
TM19	Roadway Closure Management	Future	ATMS21	Add to architecture with connection to ICM concept
TI03	Dynamic Route Guidance	Existing	ATIS04	Acknowledge the connection to the ICM concept

Source: USDOT ARC-IT National ITS Reference Architecture, Version 9.0

CONCEPTUAL REAL-TIME DATA SHARING ARCHITECTURE DIAGRAM

Figure 1 describes how data could be shared among agencies in real-time to support integrated corridor management. Notably, an ICM "Decision Support System" (DSS) is listed in the "Centers" section of the diagram. In other integrated corridor management examples across the US, DSS have been used with varying levels of automation to support the assessment of traffic situations, and the coordination and selection of appropriate response for traffic management agencies in real time. Some level of DSS is fundamental for integrated corridor management because of the direction and framework it can provide for the overlapping transportation networks that make up a corridor. While the exact specifications of a DSS will not be identified at this time, Figure 1 should inform the required functionality for real-time multi-modal data sharing.

The conceptual diagram is intended to document data flows that will help agencies better understand total person capacity when managing a corridor. This includes information on transit capacity, bus bike rack capacity, and passenger vehicle and bike parking availability in addition to passenger vehicle capacity on a corridor.

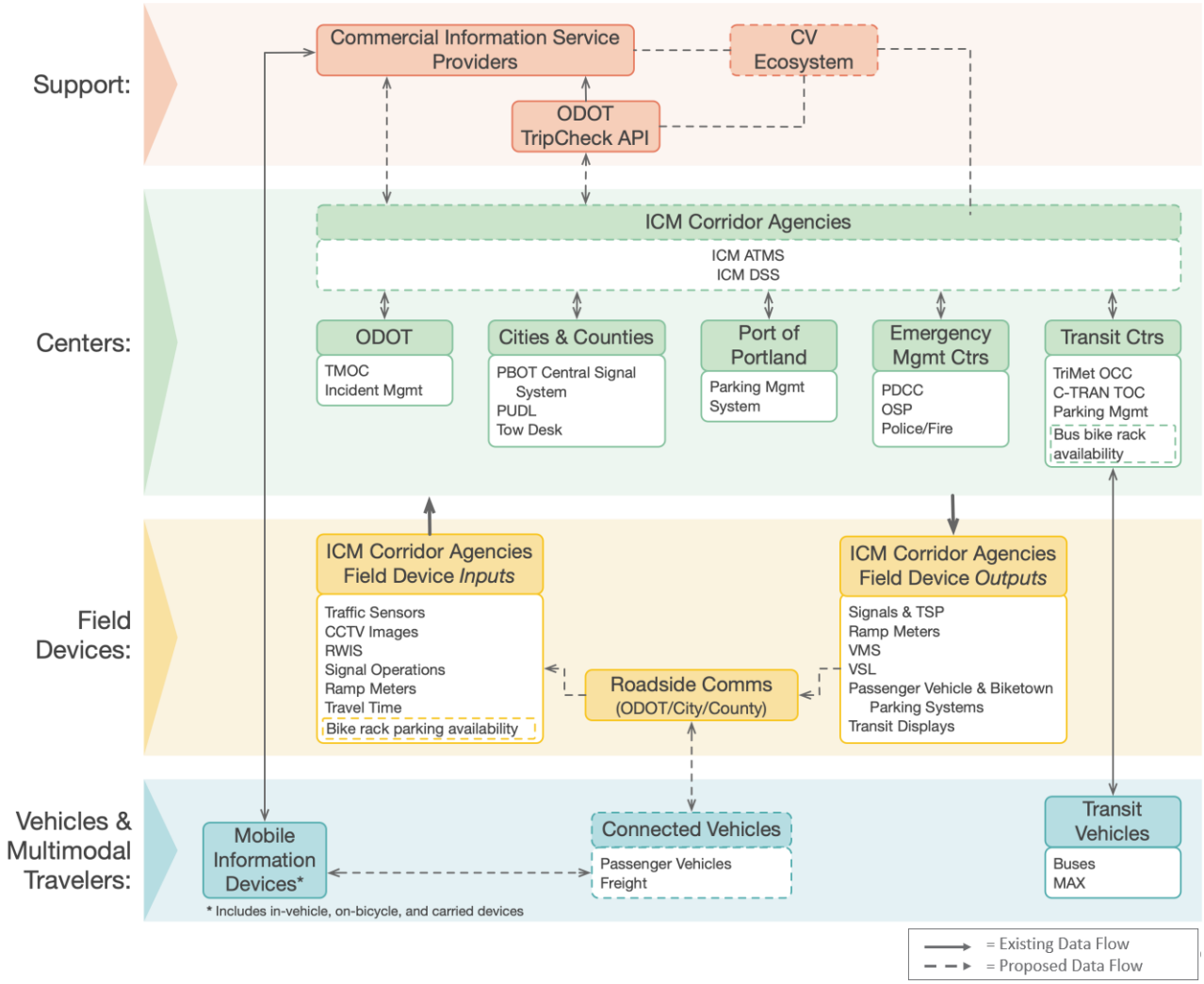

FIGURE 1. PROPOSED ARCHITECTURE FOR INTEGRATED CORRIDOR MANAGEMENT

The diagram also includes proposed connections for future transportation technology. This includes future data sharing flows between connected vehicles (both passenger and freight) and ODOT's Connected Vehicle Ecosystem.[1] Connected vehicle data (collected via the cell network or roadside communication devices) can be used to supplement the existing ICM Corridor field devices to give operators a more comprehensive view of activity on a given corridor.

CYBERSECURITY RECOMMENDATIONS

Effective integrated corridor management relies on a solid, secure Intelligent Transportation Systems (ITS) network. ITS networks have traditionally been designed, installed, maintained, and operated independently of IT networks; however, over time, the need to share data within an agency and with other entities has required the two to be connected. Transportation agencies have also leveraged database, application, server, and storage expertise that already existed in their IT departments as ITS has become more reliant on data and analytics. This section provides several cybersecurity recommendations for ODOT and Metro to consider when implementing integrated corridor management.

PHYSICAL ATTACKS

Physical security is one of the most important concerns for ITS networks. ITS infrastructure is physically accessible on roadways and is in areas where the public is expected to be. Intruders may want to gain physical access to remote ITS equipment to access network ports, access stored data, exploit vulnerabilities, and more. Mitigation of physical attacks is critical for the success of integrated corridor management. Table 2 lists a set of mitigations.

TABLE 2. MITIGATIONS FOR PHYSICAL ATTACKS

MITIGATION AREA	MOST EFFECTIVE MITIGATIONS
TAMPER RESISTANCE	• Hardened enclosures • Locks • Security hardware • Fencing/encapsulation
TEMPER EVIDENCE	• Seals • Security tape
DETECTION	• Log when cabinets or enclosures are opened • Triggers for response
RESPONSE	• Formalized, documented, exercised response • Staff or automatic (alerts to staff, disabling equipment/network)

[1] ODOT's Connected Vehicle Ecosystem is currently being implemented.

WIRELESS ATTACKS

Wireless attacks on ITS networks can be conducted to gain access to the ITS network or make the network unusable. The following guidelines are important for securing wireless transport networks:

- Ensure all equipment has up to date firmware and security patches
- Use all aspects of physical access security when possible
- Use licensed frequencies when possible

NETWORK ATTACKS

Network attacks can include targets to the Communications Layer, Services Layer, or Data Services Layer. Attacks on ITS network infrastructure commonly occur due to a physical security failure, so ITS networks should implement network security assuming someone has gained physical access. Table 3 provides a set of network security recommendations.

TABLE 3. NETWORK SECURITY RECOMMENDATIONS

RECOMMENDATION AREA	RECOMMENDATIONS
GENERAL	• Use switch port security which will only allow access to the network for the known, connected equipment • Log all network changes and port status changes, where any intrusion should generate an alert to staff or an automated response • All empty ports should be disabled • When possible, network access from one remote site to another remote site should not be possible unless there is an operational need
INTERNAL TO THE AGENCY	• Access to the ITS Network should only be possible for systems and users who have an operational need to access the network
REMOTE ACCESS	• Remote access should be provided by the IT department of the agency and conform to their IT security policies

TECHNICAL CAPABILITIES NEEDED

Several technical lessons learned identified by FHWA[2] should be considered when implementing integrated corridor management with multimodal data feeds:

[2] FHWA Integrated Corridor Management Implementation Guide, Detailed Design Lessons Learned

- Use communication standards to enable integration of central software and field equipment from different manufacturers.
- Use open-source data and code so that upgrades to the any systems are accessible by all stakeholders.
- Document and share legacy systems, versions, and capabilities from the start so that all stakeholders know exactly what each jurisdiction is running.
- Consider integrating multiple data sources for the same data to prepare for when a particular data source is not available.
- Have signal systems with the same or similar operating potential to improve the effectiveness of overall ICM.
- Have demonstrations of prototype systems early to ensure the system meets operator needs and requirements.
- Stay in touch with individuals that have the data feeds and technical knowledge about those feeds. Automate data feeds into the ICM when possible so that one system can be used to access all information needed.
- Translate data schemes to be harmonized on one base map and document translation tables to verify accuracy.
- Controls on the system (e.g., IT policies for the number of system login failures) should be harmonized across agencies.

SECTION 3: DATA SHARING POLICY LANGAUGE

DRAFT POLICY LANGUAGE, UPDATED SEPTEMBER 2021

DRAFT INTEGRATED CORRIDOR MANAGEMENT POLICY FRAMEWORK:

This section presents the proposed policy language for transportation data sharing that will support integrated corridor management. The following sections present the proposed policy language, and additional detail on the roles and responsibilities that are essential for supporting this transportation data sharing policy.

PROPOSED POLICY LANGUAGE

Real-time data sharing for agencies, transportation operators, and travelers supports the ability to proactively manage demand and capacity across all modes of travel during recurring and non-recurring congestion. Sharing real-time data through a consistent and reliable system empowers transportation infrastructure owner-operators to cooperatively maximize the efficiency and safety in a corridor. This policy is intended to support the operation of safe, multimodal, integrated, reliable, and efficient corridors throughout the state, where the focus is on the transportation user and equitably sharing the economic and quality of life benefits.

This policy language is grounded in a higher-level planning process that emphasized agency collaboration and partnership to understand the most important elements of a data sharing policy.

ALIGNMENT WITH EXISTING POLICIES

Sharing real-time data to support integrated corridor management directly aligns with the following regional polices in the Portland Metropolitan region:

- Portland Metro's 2018 Regional Transportation Plan, TSMO Policy 2: Expand the use of access management, advanced technologies and other tools to actively manage the transportation system.
- Portland Metro's 2018 Regional Transportation Plan, TSMO Policy 3: Provide comprehensive, integrated, universally accessible real-time travel information to people and businesses.
- Portland Metro's 2018 Emerging Technology Strategy, Policy 3: Use the best available data to empower travelers to make travel choices and to plan and manage the transportation system.
- Oregon Department of Transportation's 2006 Oregon Transportation Plan, Policy 2.1: It is the policy of the State of Oregon to manage the transportation system to improve its capacity and operational efficiency for the long term benefit of people and goods movement.
- Oregon Department of Transportation's 2006 Oregon Transportation Plan, Policy 5.1: It is the policy of the State of Oregon to continually improve the safety and security of all modes and transportation facilities for system users including operators, passengers, pedestrians, recipients of goods and services, and property owners.
- Oregon Department of Transportation's 2006 Oregon Transportation Plan, Policy 7.1: It is the policy of the State of Oregon to work collaboratively with other jurisdictions and agencies with the objective of removing barriers so the transportation system can function as one system.

The following section will provide supporting language for the roles, responsibilities, and processes that are essential for data sharing to support integrated corridor management.

Disclaimer: The policy language in this document are not politically invested policies, rather they are intended to be refined until we have agreed upon procedural policies for data sharing to operate a multimodal integrated corridor management.

ROLES

This section describes the roles related to the formation of ongoing regional transportation data sharing. Each agency involved in integrated corridor management should follow the principles detailed in this section.

Regional Alignment

Activities related to integrated corridor management should align with regional visions and policies on data sharing.

Usage

Agencies using data to support integrated corridor management and dispersing traveler information should state their intent to use the data prior to doing so to ensure transparency and prevent liability concerns.

Stewardship

Agencies will provide structured access to transportation data and/or actively publish data to a central repository. The rest of this policy will refer to the "central repository" to capture both structured access and/or centrally stored data that connect the information flows of the ICM Architecture.

RESPONSIBILITIES

This section describes the responsibilities for contributing to, managing, operating, and maintaining a regional transportation data sharing system.

Interagency Responsibility

Agencies sharing and using data have a responsibility to one another to support successful integrated corridor management. One agency may be responsible for the centralized repository while partners are responsible for contributing data and all are responsible users of the data.

Administration

The agency responsible for the centralized repository must be prepared to continuously manage and provide access to the repository.

Maintenance

The agency that houses the centralized repository is responsible for maintaining the agreed upon information flow availability. Other agencies contributing data to the central repository are also responsible for maintaining the data they share that others depend on.

Liability

Agencies are liable for any decisions that are made using data from the centralized repository.

Accountability

Agencies sharing data with the centralized repository must commit to an established and agreed upon level of data quality before being permitted sharing access.

Timeliness

Real-time data within the centralized repository must be collected, distributed, and archived in a frequency that is supportive of integrated corridor management. "Real-time" data for this purpose shall be delivered in a frequency to allow agencies to make transportation management decisions in rapid reaction to incidents and major events.

PROCESS

This section describes the processes that should be followed to maintain the integrity of data sharing for integrated corridor management.

Standards

Use standardized data according to established data rules, requirements, and guidelines for consistency.

Metadata

Time-stamped metadata shall be provided for each data set integrated into the central repository. Any updates to data format shall be documented and made available for anyone accessing the repository.

New Data Sources

Data sources that are integrated into the centralized repository must conform to the established standards of the repository. Any necessary translations to the data must occur prior to entering the repository in advance of being permitted data sharing access.

Agreements

Before using or sharing data within the centralized repository, agencies or other data providers must agree to conform to the established data rules, requirements, and guidelines for consistency.

Security

Data streams and central repository security must conform to the IT policies of the responsible agency. Additional cybersecurity measures may be established to protect the real-time transportation data privacy.

Transparency

All agencies using and sharing data to support integrated corridor management should communicate the use of shared data and resulting benefits with other agencies and the public. This communication should also detail the established privacy measures, welcome feedback and provide timely responses.

Publication

A pre-established level of information shall be produced for the public as real-time traveler information. This output should be agreed upon by all agencies and data providers sharing their data with the repository.