TxDOT Statewide TSMO Technology Solutions

February 2021

Version 1.1

Prepared By

AECOM Imagine it. Delivered.

Table of Contents

List of Tables

List of Figures

DOCUMENT CONTROL		
Date	Version	Description
9-8-20	1.0	Traffic Safety Division Review (Prepared by AECOM)
11-19-20	1.1	Version addressing TxDOT revisions
2-09-21	1.2	Version addressing minor formatting edits.

List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
API	Application Programming Interface
ATMS	Advanced Traffic Management System
AWS	Amazon Web Services
CAD	Computer-Aided Dispatch
CAT	Cooperative Automated Transportation
CCTV	Closed Circuit Television
CRIS	Crash Records Information System
DIIMS	Development, Integration, Implementation, and Maintenance Services for Traffic Management Systems
DOT	Department of Transportation
FHWA	Federal Highway Administration
GIS	Geographic Information System
IP	Internet Protocol
ISO	Information Security Officer
IT	Information Technology
ITD	Information Technology Division
ITS	Intelligent Transportation Systems
ITTL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
MTTR	Mean Time To Repair
NCM	Network Configuration Manager
NOAA	National Oceanic and Atmospheric
OEM	Original Equipment Manufacturer
TMC	Transportation Management Center
TAMS	Traffic Asset Management System

Acronym	Definition
TIM	Traffic Incident Management
TRF	Traffic Division
TMS	Traffic Management System
TSMO	Transportation Systems Management & Operations
TxDOT	Texas Department of Transportation

1. Introduction

In recent years, the Texas Department of Transportation (TxDOT) has adopted an approach of "spreading a culture of data" with a goal of delivering the right information to the right user at the right time to optimize decisions, enhance efficiency, and accelerate results.

As Transportation Systems Management and Operations (TSMO) continues to change the way Departments of Transportation (DOT) do business, DOTs are finding it a necessity to stay current on the latest trends in the technology industry in order to maintain existing technology solutions and equipment and plan for the future.

Technology is a topic featured at professional conferences such as ITS America and ITS Texas. ITS Texas is an annual gathering of industry experts and leaders who meet over a three-day period to discuss current topics and trends across all aspects of the transportation industry. Vendors are invited to bring their latest innovations for demonstration to TxDOT, consultants, and contractors. The forum offers an opportunity for TxDOT employees to share information across divisions and districts and provides a platform for TxDOT employees to gain insight into new technologies to help plan for the future. Contractors and leaders in the industry are invited to give lectures and hold work groups to discuss industry trends and different ways to solve problems common to all DOTs.

The purpose of this technical memorandum is to support TxDOT's Traffic (TRF) Division in providing TSMO input to the Information Technology Division (ITD), Enterprise Work Groups, and other Innovation Committees within the Department regarding statewide technology solutions for various needs, such as asset management, network management, software management and upgrades, cyber security, and performance measurement.

2. Asset Management

Asset Management plays a critical role in the success of a TSMO program by enabling more efficient tracking, management, and response to daily tasks. The system should include a network management system that can be utilized not only by Transportation Management Center (TMC) and Maintenance staff but also by other TxDOT Division and District staff (e.g., roadway and bridge maintenance; facility maintenance, fleet maintenance, procurement, project management).

2.1 Functions

An effective Asset Management System has the capability to empower TxDOT's TSMO staff by streamlining work order management, optimizing preventive maintenance tasks, and generating performance metric reports. They provide ease of tracking work orders and assets digitally, making it easier to organize and view data, as well as assign appropriate labor and response resources. Costs savings and data-driven decision making are just two of the inherent benefits.

Prioritization capabilities allow for service requests and work orders to be managed more efficiently. Asset Management software can provide immediate insight on the health status of TxDOT's Intelligent Transportation Systems (ITS) and Signals network and their associated assets (e.g., Closed Circuit Television (CCTV) cameras, dynamic message signs, vehicle detectors, controllers, communication equipment). Specifically, the system can support the following functions:

- Issuing trouble tickets;
- Dispatching maintenance staff;
- Work order tracking, management, and reporting;
- Asset management and reporting;
- Tracking costs for repairs and maintenance;
- Planning for future work or maintenance;
- ITS network device maintenance scheduling;
- Labor tracking and reporting;
- Process management;
- Project support for deployment scheduling and management;
- Network and component performance evaluation reporting;
- Signal service requests;
- Fleet maintenance management;
- Managing accounts and budgeting; and
- Facility maintenance.

A robust asset management system provides the capability to store all asset and network information in a central database for easy access and retrieval to support the health status monitoring of systems and infrastructure as well as support preventive, corrective, and emergency maintenance and technology replacement programs.

2.2 Benefits

Asset Management Systems enable the tracking of a problem from detection through resolution as well as from the implementation of a new process or project to systems acceptance. These systems also help maintain an organized process of authorization and minimize downtime for affected network devices throughout the life of the ticket(s)/project. Asset Management Systems also help one become accountable for their share of responsibility in strengthening the overall network's performance and function. Having the ability to pull mean time-to repair metrics, past trouble history, performance data, and location information, along with detailed and customizable reports all with a couple of clicks saves significant time that could otherwise be spent working on the optimization of TxDOT's TSMO assets. Specifically, the benefits of an Asset Management System include improvements in:

- Work order and service request management;
- Task management, work process flow, assignment, and accountability;
- Asset and inventory management;
- Statistical reporting of assets and state of the TSMO systems and infrastructure;
- Reliability and reduction of downtime;
- Planning and scheduling of all maintenance and upgrades of assets;
- Cross-division communication; and
- Overall efficiency through sustainable asset management operations.

2.3 Needs

While the systems engineering process should be applied to define the specific requirements of TxDOT's Asset Management System, the following needs should be addressed as a minimum:

- Interactive map displaying current information on field devices (e.g., location, status, icon for device type);
- Database for storing historical data for assets including name, manufacturer, model, Internet Protocol (IP) address, pictures, location data (i.e., latitude, longitude, roadway, cross street), and maintenance history;
- User interface that is intuitive and easy to navigate;
- Ability to drill down to assets from the map and integration with Geographic Information System (GIS) tools;

- Graphic displaying calendar view of scheduled work orders;
- Report functionality that allows for customizable reports;
- Capability to run on multiple platforms including Windows desktop/laptop, toughbooks, and mobile devices such as cell phones (iPhone and Android) and tablets;
- Labor and materials management to track labor and material costs; and
- Tracking preventive maintenance work orders.

2.4 Products

There are many Asset Management systems available in the commercial market that provide basic functionality for tracking assets. Some of the more common systems that are used in the ITS industry include the products described below.

Cartegraph

Cartegraph is a cloud-based Operations Management system that utilizes web technologies and employs a wide range of functionalities including:

- Tracks vehicle costs per hour or per mile;
- Takes work requests from internal/external sources;
- Creates custom reports;
- Able to use electronic methods (tablets, smart phones, laptops) to receive, close out, and request work orders;
- Able to create vehicle replacement ratings;
- Creates weighted conditions; and
- Able to integrate with various software packages.

Cartegraph allows users to layer various maps. While Cartegraph is a business partner with ESRI, their system comes standard with Google Maps. Virtually every screen contains a map. Cartegraph has developed a simplified interface that helps users to enter information accurately and consistently. The system is placed in the cloud enabling work in real-time on multiple devices with visuals on most screens.

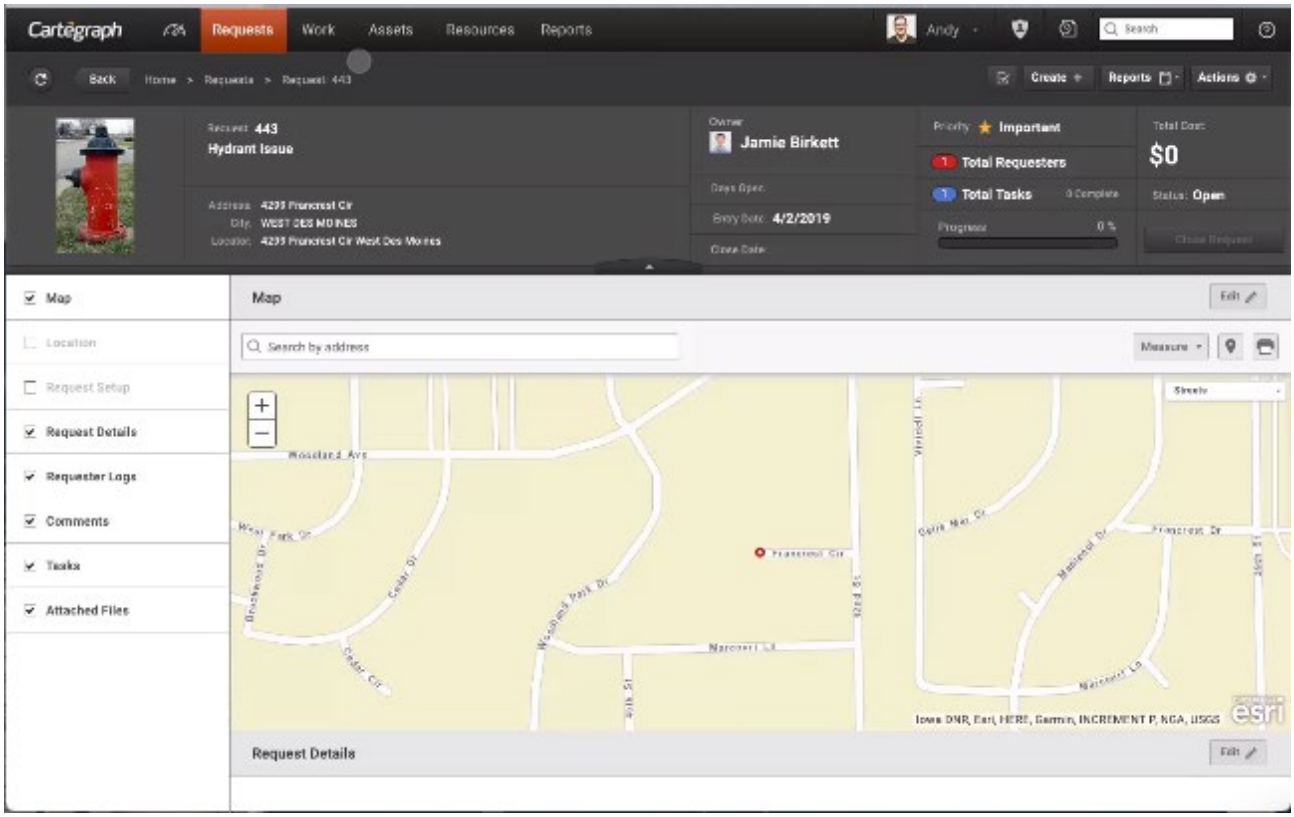


Figure 1: Cartegraph System Screenshot

Cityworks

Cityworks does not contain separate asset tables that need to be integrated, synchronized, or linked to the GIS. The GIS offers a robust and accurate representation of an organization's assets. Data models are user definable and non-proprietary, making this information usable with other applications. No interface, integration, or synchronization is required as there is only one common asset database. The software is built on ESRI ArcGIS Server technology to empower users to leverage GIS to manage their organization's assets. Cityworks Server enables a wide variety of organizations to manage their capital assets, infrastructure, and automates these work processes:

- Call Center;
- Service Requests;
- Work orders, including cyclical/preventive maintenance work;
- Inspections, tests, and condition assessments;
- Resources, storerooms, projects, and contracts;
- Reports and dashboards;
- Mobile workforce; and
- Interfacing to other systems (accounting, billing, etc.).

The Cityworks Server incorporates a palette of tools, tabs, and links in a highly customizable environment, allowing it to be deployed as an intranet application across a district, division, or the entire organization.

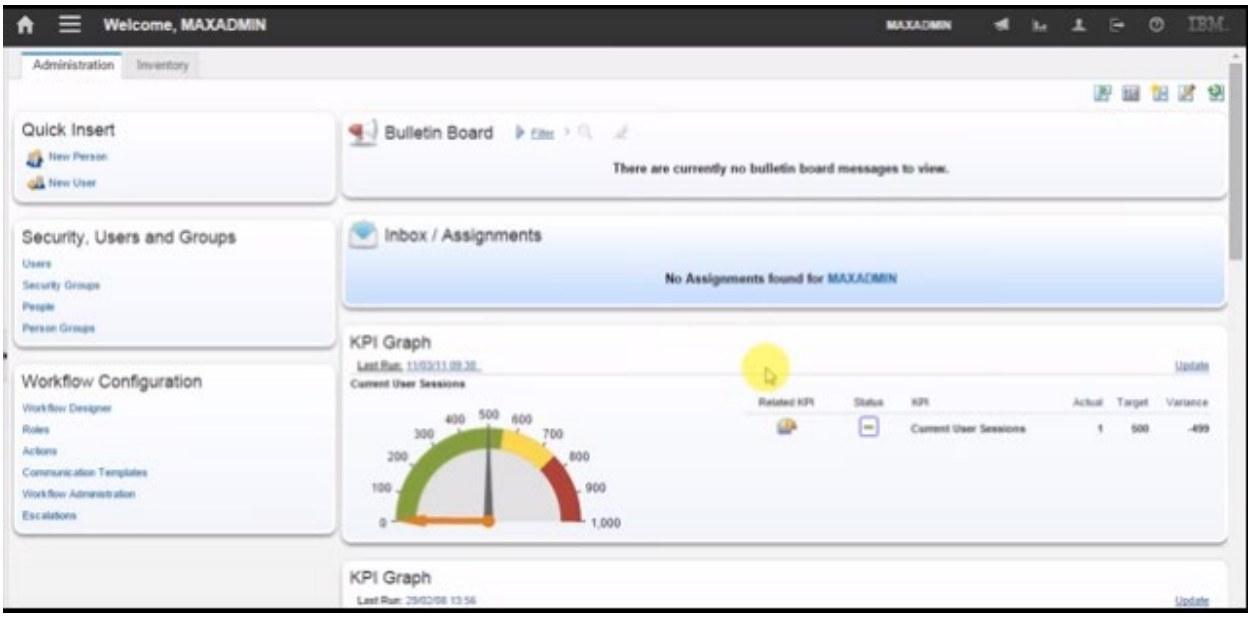


Figure 2: Cityworks System Screenshot

IBM Maximo

IBM Maximo Asset Management is used to plan and execute maintenance activities for multiple asset types, as well as to keep track of information on asset costs for companies operating in any industry. Focusing on asset maintenance, optimization and service delivery, this product helps ensure maximum return on assets by reducing costs and increasing asset uptime. It facilitates the development of a coordinated program for preventive, predictive, routine, and unplanned maintenance. Advanced scheduling functionality allows deployment of personnel with the appropriate skills at the right time.

This product consists of six key management systems that enable management of assets, including production equipment, facilities and transportation assets, in alignment with their business objectives. These six management systems include:

- Asset management;
- Work management;
- Service management;
- Contract management;
- Materials management; and
- Procurement management.

IBM Maximo Asset Management can optimize performance while managing the complete lifecycle of critical assets including planning, procurement, deployment, tracking, maintenance and retirement. This translates to more timely and accurate data collection, reduced operating costs, and increased maintenance productivity.

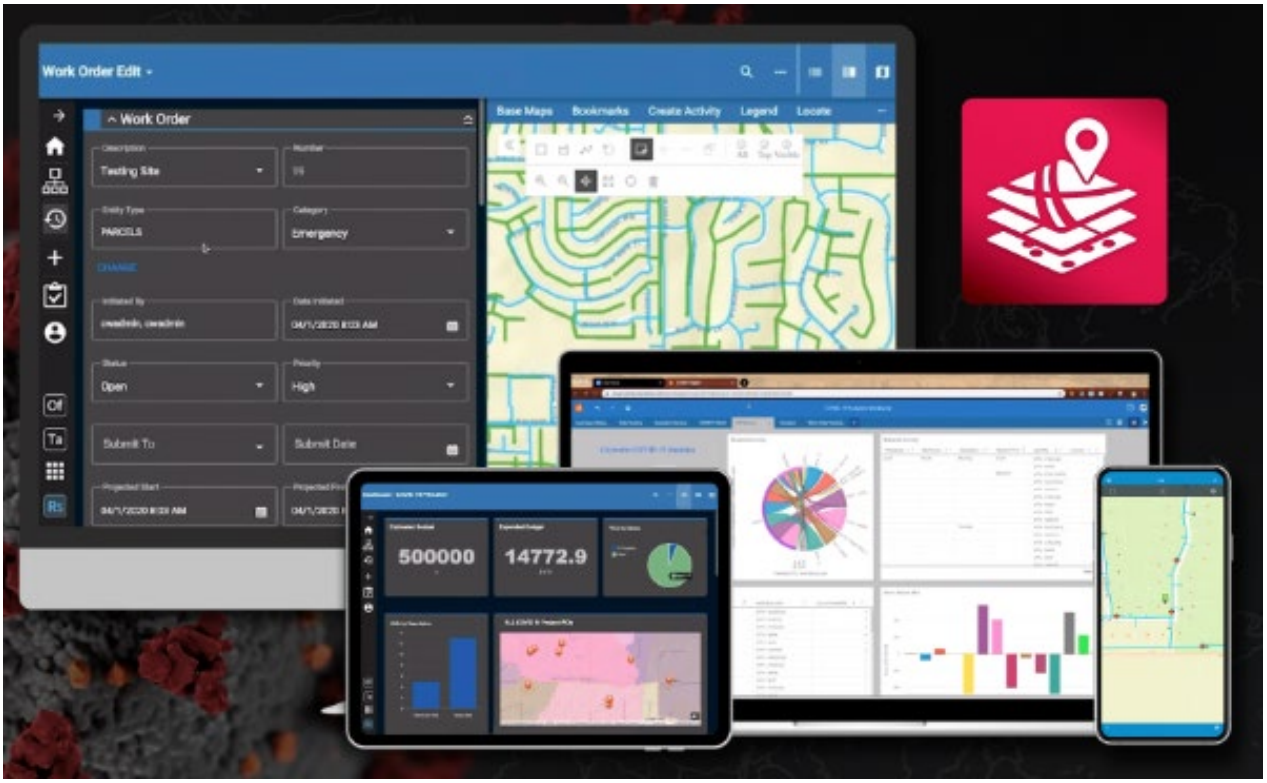


Figure 3: IBM Maximo System Screenshot

Asset Works

Asset Works develops original and historical costs of fixed assets and infrastructure. By inventorying capital assets and tagging equipment with barcodes, Asset Works implements fixed asset systems to develop and maintain proper stewardship of assets. Their services provide both initial and long-term benefits addressing:

- Financial reporting;
- Grant compliance reporting;
- Infrastructure inventory & valuation;
- Property insurance;
- Property control & management;
- Valuation and inventory record perpetuation; and
- Annual updating of values.

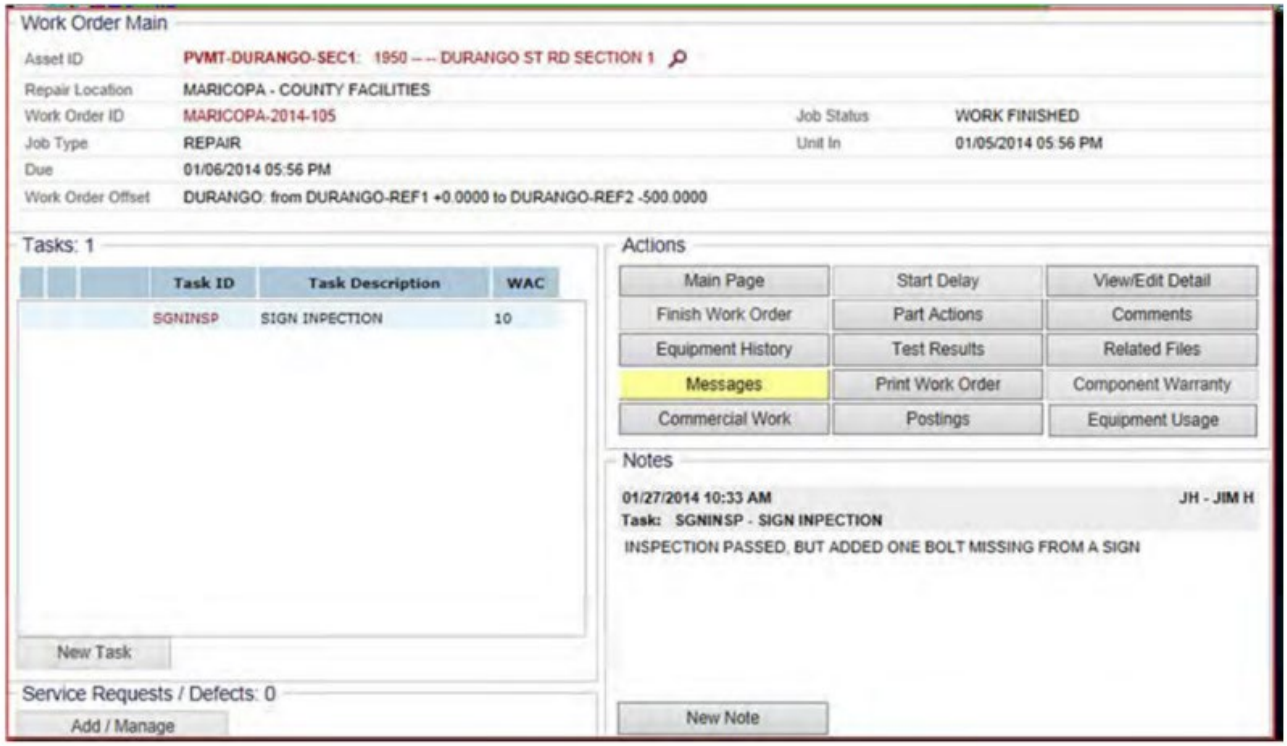


Figure 4: Asset Works System Screenshot

A typical engagement involves compiling asset inventories, inventory valuation, and barcode asset tagging, developing property control procedures, drafting reports, and implementing technology solutions.

2.5 TxDOT's Current Asset Management System

ServiceNow is an Asset Management software application that TxDOT began using for tracking trouble tickets during 2014 and is now using it for tracking district ITS and signal assets. These assets include CCTV cameras, dynamic message signs, vehicle detectors, and signals. It appears that the following are limitations of the system:

- It is not an asset management system commonly used by DOTs;
- Few options exist for preventive maintenance reporting (i.e., tickets only);
- Need to build out all database tables for ITS devices; and
- Does not include asset receiving.

ServiceNow is hosted on a cloud server system (TxDOTNOW). It recently added a map interface, although TxDOT is not using it yet. Incident tickets are submitted and converted to work orders. District staff are being trained on how to use the system by ServiceNow personnel. ServiceNow has the following plugins:

- Asset Management Model (Fort Worth pilot program in 2017);
- The Pharr and Laredo districts use it for roadway luminaire repair, signals on flash, and maintenance;
- Field Service Model: Map IF just introduced in Orlando, TxDOT not using yet;
- Preventive Maintenance Module – not currently being used;
- Reporting needs to be set up, can export to excel; and
- Mobile phone app.

2.6 Recommendations

The following recommendations are provided based on a cursory review of available Asset Management systems and their features compared to the existing Asset Management system currently being used by TxDOT:

- Apply the Systems Engineering process to develop a Concept of Operations and system requirements for either enhancement or replacement of the ServiceNow system.
- Consider expanding the scope of the Asset Management system to include both system and infrastructure assets such as roadway pavement, bridge structures, guardrail, luminaire, signage, pavement markings, drainage, and other assets.
- Conduct a comparative analysis of alternative Asset Management systems, including others not mentioned in this report, and select a system based on best value considering compliance with system requirements and price.

In summary, Asset Management plays a critical role in achieving high levels of asset uptime and system availability to support the goals of the TSMO Program. A robust asset management system provides the capability to manage asset information more effectively in a central database for easy access and retrieval to improve the quality of operations and maintenance in a cost and schedule efficient manner.

Recommendations: ServiceNow, in combination with SolarWinds, will be expanded to monitor ITS and signal assets in all districts by the end of 2021. The following enhancements to this system should consider be considered:

- Interfacing ServiceNow with a funding component to forecast budgetary needs for life cycle maintenance and replacement of equipment;
- Interfacing ServiceNow with other civil asset management systems (e.g., roadway, bridge, and facility assets);
- Developing a map display for current information on field devices (e.g., location, status, icon for device type);
- Developing a database for storing historical data for assets including name, manufacturer, model, IP address, pictures, location data (i.e., latitude, longitude, roadway, cross street), and maintenance history;
- Providing the ability to drill down to assets from the map and integration with GIS tools;
- Developing a graphic display calendar to view scheduled work orders;
- Providing the capability to run on multiple platforms including Windows desktop/laptop and mobile devices such as cell phones (iPhone and Android) and tablets; and
- Providing the ability to track labor and material costs and preventive maintenance work orders.

3. Software Management and Upgrades

Lonestar™ is TxDOT's Advanced Traffic Management System (ATMS) software connecting TMCs with ITS field devices such as vehicle detectors, dynamic message signs, and CCTV cameras. It has the ability to monitor traffic and manage events through applications such as Event Management, Travel Time Application, and an ESRI-based Map User Interface. Lonestar™ enables operational control of these devices and reports their health, status, and any operational data or responses back to the software, which sends commands and requests to the ITS field devices. Lonestar™ software makes real-time data received from devices available to all other processes via the command and status distribution process. It is an integrated system that includes plug and play subsystems and applications depending on the needs of the districts.

The Lonestar™ database contains configuration and other pertinent information about device identification, location, and communication parameters as well as other details of how the software should behave. Lonestar™ has a center-to-center interface for districts to share data on a statewide public website; external systems provide live traffic data in lieu of field devices as well as providing a channel to send information out for dissemination. The software integrates these devices and data interfaces in many ways that are useful to other operations. Lonestar™ has several software processes that are not device specific to process data and make it usable for various operations. The Contact Notification Application, Travel Time Application, and Event Management Subsystem are examples.

3.1 Software Maintenance and Upgrades

The Lonestar™ ATMS has been in existence for approximately 20 years and is maintained with software upgrades through the "Development, Integration, Implementation, and Maintenance Services for Traffic Management Systems" (DIIMS) contracts. The Florida DOT SunGuide® ATMS and TxDOT Lonestar™ ATMS are similar in purpose, design, and implementation; however, is not adequately compatible to directly share system components. Over the years, both agencies have made enhancements to their software systems. Some enhancements have been funded and built by one agency and then shared with the other agency. The effort involved in taking an enhancement that has been completed and deployed and making it available to another agency can be substantial. This is due to the ATMS software products maturing in slightly different directions; however, both DOTs are interested in maintaining a collaborative relationship to build on their successes and their assets, and achieve the capability to share system components and enhancements, and thus share the burden of development and maintenance of the software.

Lonestar™ ATMS upgrades are planned on a periodic basis and include major, minor, and patch releases. A formal Acceptance Test Plan is performed in a controlled test environment at TxDOT's Cedar Park facility for all major software releases. Testing is conducted by the DIIMS contractors and includes test plans for regression testing of existing software, new functionality, and issue verification.

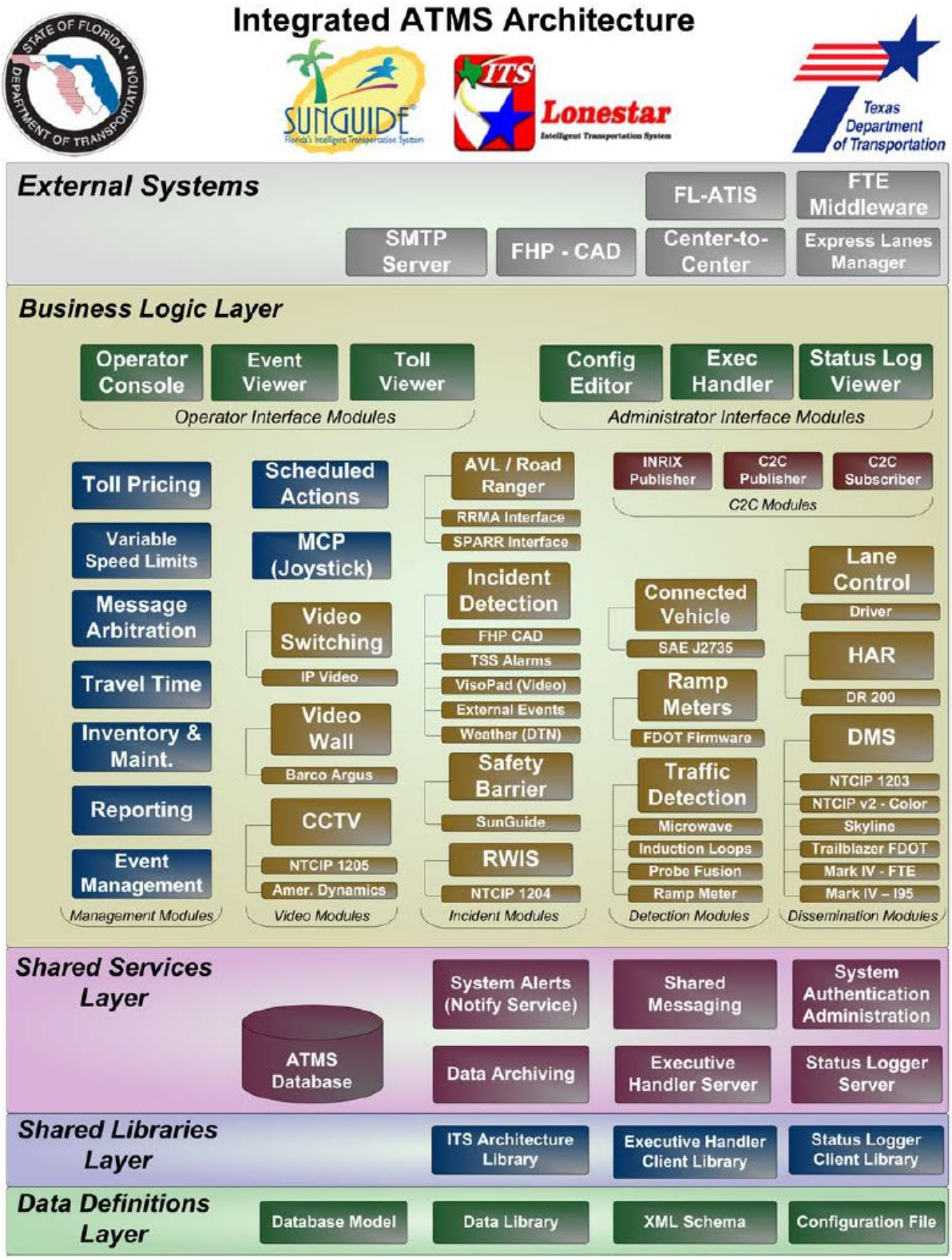


Figure 5: Lonestar™ Integrated ATMS Architecture

3.2 Lonestar™ ATMS Assessment

In April 2020, an anonymous on-line survey was conducted by TxDOT, to gather information from TMC operators about existing operational tools. A total of 24 (out of 40) TMC operations staff responded to the survey to provide insight into their operational needs. This effort, in addition to future operator interviews, will help TxDOT address these needs to develop and enact a vision for future operational tools. Table 1 shows a summary of findings from this survey.

Table 1: Lonestar™ ATMS Software Survey Findings

Strengths	Weaknesses	Suggested Improvements
Easy to use with good mapping interface	Frequent crashes, upgrades don't always fix issues in a timely manner	More control over remote CCTV access between metro & rural areas
CCTV easy to use and provides snapshot images in other districts	CCTVs inability to view all roads and affected traffic lanes	Improved mapping interface
CCTV ability to view incidents in real time	Inability to download data and generate operator specific reports	Ability to view older reports and run individual reports on operators
Fast connection to DMS and quick confirmation of posted messages	Inability to operate CCTVs remotely or edit device from rural districts	Real time traffic information for better incident management.
Easy to view and coordinate events with TMC operator accountability	User interfaces are not consistent across all subsystems and applications	Develop predictive and real time analysis for mitigating incidents

In addition, TxDOT is working on consolidating district Lonestar™ deployments into a single cloud-based system using Amazon Web Services (AWS).

3.3 Tableau

TxDOT is using Tableau to create dashboards for tracking Key Performance Indicator (KPI) metrics based on data stored in its AWS Data Lake repository. Tableau is a data visualization tool used in the Business Intelligence industry. It helps in simplifying raw data into an understandable format. Data analysis and visualizations created are in the form of dashboards and worksheets. The data that is created using Tableau can be understood by professionals at any level in an organization. It also allows a non-technical user to create a customized dashboard. Tableau is being rolled out to TxDOT staff to empower users, increase usage, and drive data culture. Data is being collected from a variety of sources including Lonestar™, Crash Records Information System (CRIS), and Traffic Asset Management System (TAMS) for the Houston District. The following three KPIs are being tracked for the metro and coastal districts on a monthly basis: Traffic Management System (TMS) Asset Uptime, Average Incident Clearance Time, and Level of Travel Time Reliability.

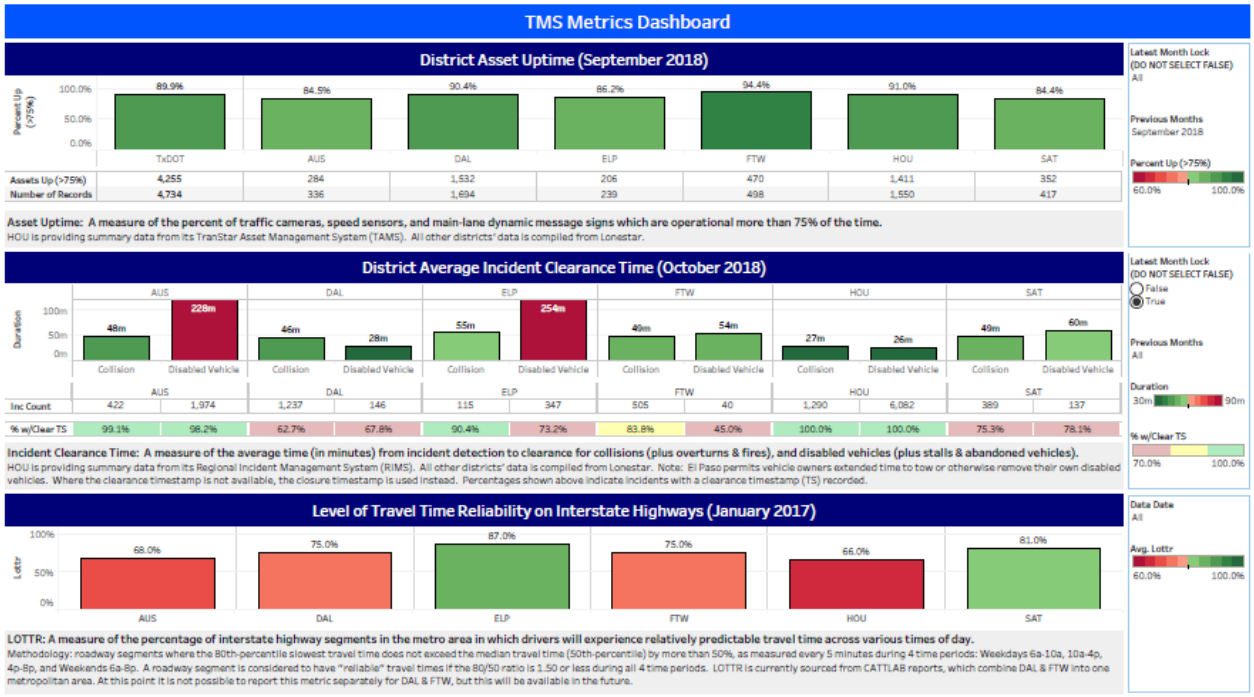


Figure 6: Traffic Management System Dashboard

3.4 Recommendations

The following preliminary recommendations are provided contingent on the completion of the Lonestar™ ATMS survey that is currently being conducted:

- Complete the Lonestar™ ATMS Assessment and schedule software upgrades to address needs.
- Apply the Systems Engineering process to develop a Concept of Operations and system requirements for the next generation of TxDOT's ATMS software.
- Conduct a comparative analysis of alternative ATMS software, including Lonestar™, and select a system based on best value considering compliance with system requirements and price.

In summary, the ATMS software plays a critical role in TMC operations to support the goals of the TSMO Program. Software upgrades should be developed and implemented to align with TSMO goals, including performance management, to drive continuous improvement in operations.

Recommendation: It is recommended that TxDOT move off the business network and onto a separate traffic network to avoid similar impacts resulting from the recent ransomware event. In addition, TxDOT should develop and implement a structured plan for Lonestar™ ATMS redundancy. This will require failover capabilities by pairing districts to be on the same version of Lonestar™ as well as normalization of each District's database to establish consistency. Such consistency will need to be continuously maintained which is a significant effort and needs to consider latency impacts in application among districts. In addition, a Lonestar™ Software Users Group representing the needs of the districts should be established to present their requests to a statewide Configuration Management Board for approvals and follow-up implementations of upgrades and enhancements.

4. Traffic Network Monitoring and Management System

In 2018, TxDOT retained the contractor Skyline Technology Solutions to develop a Traffic Network Monitoring and Management system (Reference 1). The objectives of the system are as follows:

- Improve the reliability of the Traffic Network by increasing asset uptime.
- Reduce District staff's burden of keeping equipment in good repair through remote support.
- Improve the visibility of the Traffic Network to improve longer term strategic planning.
- Improve security of the Traffic Network through centralized device security controls; vulnerabilities being identified; remediation plans being implemented remotely; and alerting when satellite buildings are accessed.

Success of the system is based on the integration of people, processes, and technology. Training and adoption of tools, systems, and processes are being implemented. This includes remote support to reduce incident management support, and proactive maintenance. Business and Information Technology Infrastructure Library (ITIL) processes create efficiencies and consistency with work output. Consistent tools are being deployed for Network Monitoring and Service Management. Today, TxDOT monitors TMS devices and has a complete view of both its traffic and business networks enabling TxDOT to enhance device uptime, improve overall performance, traffic, and safety. This enables better network visibility to improve performance reliability and long-term capacity planning. Before the SolarWinds pilot, the district had no effective monitoring system to understand the status of its CCTV cameras, dynamic message signs, or the network infrastructure supporting these devices.

TxDOT applied this network monitoring system in the Dallas district as a pilot program. This reduced the district staff time remediating network issues and improving ITS network security. Prior to the pilot, Dallas district personnel spent large portions of their time troubleshooting issues across their ITS network. They would do manual checks of equipment, going to the webpage of each camera and checking if the camera came up and the quality of the video. They would make changes on network gear in attempts to resolve outages or drive hours to a location to check the status of a single switch or sign.

Once the Dallas pilot was live, the district gained access to live polled data in SolarWinds, a suite of alerts tailored to their needs, and a 24/7/365 network operations center. Skyline worked with the Dallas district to define their high priority devices in SolarWinds, so alerts on those devices would be high severity. SolarWinds also allowed Skyline to create dependencies among devices across the network. This prevented the districts from receiving a flurry of alerts when an upstream device went down. In the past the district would learn of a network outage and it would be an exercise of going from device to upstream device to see where it originated. Now, with SolarWinds dependencies, the staff knows the origin as soon as alerted.

In addition to implementing SolarWinds, the contractor also became the first responders to outages and alerts. This allowed them to define standard operating procedures, work instructions, and escalation paths, all with the end goal of remotely remediating as much as possible, allowing the district to spend more time on planning and projects and less time reacting to calls and outages.

As the contractor took on the remote remediation responsibilities for Dallas, it soon became clear SolarWinds® Network Configuration Manager (NCM) could help the district execute on architecture and security enhancements network wide. With NCM, the district could periodically back up network device configurations, shortening Mean Time To Repair (MTTR) when a device needed to be replaced. They could also standardize their deployment of the network protocol spanning tree, preventing looping and unexpected routing behavior. NCM also allowed the district to roll out baseline configurations and centralized authentication, creating a more controlled threat landscape.

4.1 TxDOT Business Network Pilot

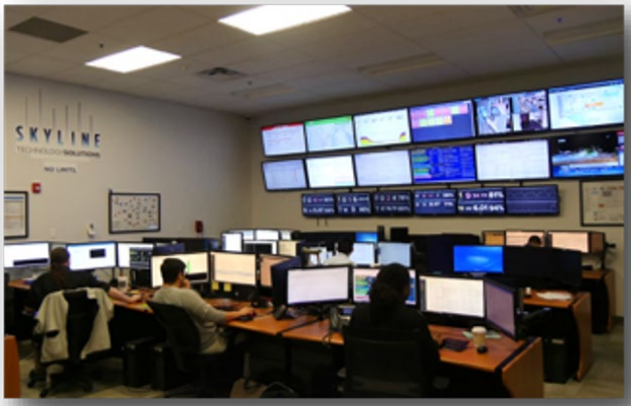
The results of the Dallas Pilot were positive where the district now has an end-to-end single view of their field devices and the network infrastructure supporting them. The goals for the Business Network Pilot were similar to those of the Dallas Pilot. TxDOT wanted to better understand the performance, capacity, resiliency, and security of its Business Network. To demonstrate the benefit TxDOT would get from leveraging SolarWinds, the TxDOT SolarWinds monitoring platform was expanded bringing on more Business Units and devices. Several districts were selected for the Business Network pilot, including Dallas, Corpus Christi, and Houston.

Dallas was selected specifically so the value of having SolarWinds monitoring the entire network, from the internal Business Network to the road-side device, could be demonstrated. The system was able to show routing paths, network hops, latency, and bandwidth to TxDOT, so long-suspected issues spanning both networks could either be validated or dismissed.

Corpus Christi and Houston were selected because they are Coastal Districts, highly likely to be affected by storms and hurricanes. During the pilot, there was a tropical depression headed towards Houston. This provided an opportunity to build a SolarWinds dashboard and accumulate all the information TxDOT needed to support their Emergency Operations Center, including a live National Oceanic and Atmospheric Administration (NOAA) map, a geographical node status map, and network availability across the districts in the coastal region.

Over three months, the contractor worked with TxDOT to rapidly iterate and demonstrate the benefits of SolarWinds centralized monitoring and management. With SolarWinds, they could quickly identify and highlight bottlenecks, identify inconsistent configurations, and show daily, weekly, and monthly trends.

4.2 SolarWinds



Based on the success of both the Dallas Pilot and the Business Network Pilot, TxDOT decided to deploy SolarWinds monitoring as a service to all of TxDOT. This required onboarding the remaining 15 Business Network districts, and the remainder of all the ITS Network districts. At the time of writing, TxDOT has the entirety of the Business Network in SolarWinds, and eight of the 25 traffic districts.

4.3 Current Status

Today, the TxDOT's Traffic and Business network devices and performance are monitored, and operations dashboards allow management to understand network uptime at a glance. TxDOT can run reports on device uptime for contractor-maintained devices vs. state-maintained devices and can determine the last person to implement a configuration change. The SolarWinds solution has helped TxDOT achieve the goals they set up during the early stages of the pilot and continue to build upon today. Other results include:

- Improved resolution rates for networking performance and capacity issues;
- Improved configuration management;
- Improved log tracking and management; and
- Increased productivity of IT staff.

Currently, the network monitoring and management system is deployed in ten districts: Austin, Dallas, Fort Worth, San Antonio, Pharr, Lubbock, Childress, Laredo, Corpus Christi, El Paso as well as the Cedar Park Lab. The system provides automated monitoring, alerting, and ticketing to accomplish the following functions:

Automated discovery and manual onboarding of Traffic Network infrastructure devices.
Automated alerts, and creation and distribution of tickets to TxDOT resources, based on rules, triggers, and thresholds.
Reboot or configuration changes that can be automated as a result of specific alerts or triggers.
Daily quality control to ensure that monitoring and ticketing are functioning properly.

In addition, changes are being made to dashboards and automated reports that allow for evaluation by TxDOT of the incident and problem tickets for future operational improvements. Coordination is being maintained with the districts to identify operational efficiencies that allow for increased scale without increased cost (e.g., remote monitoring and remediation support). As of Aug 10, 2020, a total of 8,791 TMS devices are under monitoring, approximately 65% of all traffic devices statewide, with the top ten devices listed in Table 2.

Table 2: Top 10 TMS Devices

Device Type	Count
Cellular Router	56
Detector	57
Decoder	146
Dynamic Message Sign	431
Radio	1,012
Encoder Terminal	1,060
Server	1,100
RVSD	1,152
Camera	1,675
Switch	1,780

As of January 2020, 94% of the overall devices have uptime availability. The system reduces burden of the districts by saving travel and dispatch time and costs; improving the system architecture for reducing incidents; and providing enhancements for future tracking of remote remediation. The system also improves visibility into the traffic network by helping to monitor and minimize bandwidth impacts of video sharing; plan end of life replacements; prioritize security improvements; and prioritize new equipment and configuration standards. The system improves security in the Traffic Network through inventory of assets; controlling the use of administrative privileges; securing configurations of hardware assets; limiting and controlling network ports and services; and retiring end-of-life assets.

Current expansion of the Traffic Network Monitoring and Management system is planned to continue as a district-by-district rollout of the combined Network and Asset Management solution at a pace of approximately one district per month. The next districts in the queue are El Paso, Bryan, and Tyler with the remaining districts listed in Table 3 below.

Table 3: Remaining Districts for TMS Network Monitoring Deployment

Remaining Districts for TMS Network Monitoring Deployment	
Abilene	Lufkin
Amarillo	Odessa
Atlanta	Paris
Beaumont	Waco
Brownwood	Wichita Falls
Houston	Yoakum

Based on the current deployments, positive feedback has been received by TRF Division staff. There is a wide variance of the equipment in the districts. Districts appreciate training opportunities provided by TRF and are excited about having visibility into their networks. Requests for enhancements include additional Network Training (TRF is providing); integration with ServiceNow; power pole connectivity; and a guide indicating "Who's on What Contract."

5. Cyber Security

Some of the greatest management challenges facing the public and private sectors today are from persistent and advanced cyber threats. Security breaches are an everyday threat to government agencies and state DOTs are a target for professional hackers and foreign countries to infiltrate servers, steal data, and corrupt systems. The cost of such a breach can be enormous for a company or agency to overcome including:

- Loss of system availability;
- Stolen data;
- Loss of worker productivity during system downtime; and
- Cost of cleaning and restoring the system.

Today's dynamic threat environment requires integrated solutions, aligned closely to industry-specific operations and critical business functions. The challenge is understanding potential vulnerabilities and making informed, critical decisions on what and where to budget for security and resilience of assets, systems, and networks. Cyber security is a recent focus area among Departments of Transportation and has been an area of attention during at least the last two legislative sessions in Texas. As a result, legislation has been passed, training has been mandated, and policies have been enacted.

5.1 TxDOT's Information Technology Division

TxDOT's Information Technology Division (ITD) supports business operations of the Department with innovative IT and strategic information resource planning. The division is divided into five functional areas (Reference 2):

Information Security - implements a robust information security program to protect TxDOT systems and data from cybersecurity threats; sub-sections are Risk and Compliance, Cybersecurity Operations, and Toll Information Security.

Customer Relationship Management - ensures that customer business needs are properly captured and incorporated into decision-making; sub-sections are Customer Outreach and Communications, Data Management, and Project Management.

IT Operations - plans and coordinates the delivery of IT services and products to TxDOT employees and customers while ensuring the appropriate infrastructure and application support are available; sub-sections are Application Services, Infrastructure, and Service Desk.

Vendor Management and Sourcing - provides critical oversight and management of TxDOT's contracted IT services, working closely with agency procurement to ensure prescribed process are followed; sub-sections are Vendor Management and IT Sourcing.

Financial Reporting and Asset Management - manages the division's budget and expenditures.

5.2 TxDOT Information Security Policy Manual

In November 2017, TxDOT published the "Information Security Policy Manual" (Reference 3). This manual issues policies for TxDOT's information security functions and creates a dynamic program that protects the confidentiality, integrity, and availability of TxDOT's information resources. TxDOT uses a risk management approach to balance business productivity with data and infrastructure asset protection. TxDOT's Executive Director delegates authority and responsibility for this approach to the Information Security Officer (ISO), who directs the Information Security Program. Along with the policies issued in this manual, the ISO:

- Governs the security processes to implement these policies;
- Identifies the procedures to carry out the processes;
- Establishes the standards by which implementation of the policies is measured;
- Monitors the effectiveness of each process and makes adjustments as necessary;
- Verifies that process results meet established standards;
- Validates results; and
- Reports on the Information Security program status.

The "Information Security Policy Manual" addresses policies and protocols specifically addressing the contents presented in Table 4.

Table 4: TxDOT Information Security Policy Manual Highlights

Security Awareness
Security Awareness Policy - fosters an environment where individuals can make knowledgeable decisions to keep information secure and to protect the data and systems TxDOT uses.
Using Passwords - describes how to improve the use of passwords.
Planning for Security - TxDOT's Information Security Office manages the planning process for security controls to enable business functions while managing risks. This effort links the Agency's security program with its Strategic Plan. Linking security controls with the Strategic Plan aids project teams to coordinate security concerns as they develop automated business solutions.
Acquiring Systems and Services - establishes how TxDOT reduces the inherent risks in buying information technology equipment or services by considering security controls during procurement.
Using Information Assets in an Acceptable Way - establishes how TxDOT protects its information assets from inappropriate uses to reduce risks, such as: exposures to virus attacks, compromising of network systems and services, and legal issues. As part of the Security Awareness Policy, this section lists topics to consider and behavior to avoid.
Training to Increase Security Awareness - explains how TxDOT will increase attention to potential threats, enabling individual users of Agency information resources to avoid behavior that could put its information systems at risk. As part of the Security Awareness Policy, this information provides the parameters to establish an awareness and training program.
Intrusion Prevention
Intrusion Prevention Policy - establishes a complex, layered, and overlapping approach that leverages people, processes, and technologies to monitor the environment, assess threats, and identify weaknesses. The intent of the policy is to protect information assets by verifying that individuals have authorized access and by preventing intentional and accidental use of TxDOT information throughout its lifetime, regardless of its location.
User Identification and Authentication – addresses identification of individuals to verify their identity before allowing access to its information assets.
Access Control - Controlling access into a system (internal or external to the agency, wired or wireless, on premises or remote) provides necessary protection for information assets and the environment in which they reside. There are multiple ways to protect these points of entry. Commonly known as access controls, these protections allow entry only to individuals or systems with prior approval who have a declared need, and to whom access has been extended. TxDOT uses multiple tools in various formats - physical and virtual locks - to authorize entry.
Perimeter Control - Much as a fence with a locked gate can control who goes in or comes out of an area, a secure perimeter around TxDOT's network can reduce the exposures of unwanted intrusions. Both, physical

or virtual fences, must have the proper configurations to keep out trespassers. TxDOT is committed to reducing its exposure to potential threats while ensuring authorized individuals have the functionality necessary to perform legitimate business. This section establishes how TxDOT will control its perimeter as part of its Intrusion Prevention Policy and describes the minimum requirements that must be in place to regulate access to its network.

Security Monitoring - Monitoring and logging all security events and incidents provides TxDOT the ability to recognize, react to, and mitigate actions that threaten to disrupt the availability and integrity of TxDOT information assets.

Internet Content Filtering - The inherent risks of conducting state business over global, public networks reinforce the need for careful, deliberate filtering of Internet content. This content includes email, telephony, video, web services, web browsing, and file transfers.

Vulnerability Assessments - All TxDOT information systems undergo vulnerability assessments to help and correct flaws that leave them open to attack. This specifies how often these assessments are conducted and how their findings are addressed.

Cloud Usage - Selecting the appropriate virtual environment for computing resources is the first critical step in procuring secure cloud services. Cloud services includes both the hosting of content on a virtual network and accessing the service through an Internet connection.

Information Protection

Information Protection Policy – ensures a balance between using information and protecting its quality and integrity to allow for the optimization, maintenance, and disposition throughout the information's lifetime.

Classify Data - establishes how TxDOT classifies data as part of its Information Protection Policy and describes the minimum protocols and responsibilities that must be in place to effectively assess the value of information against the risk of it being misused.

Encrypt Data - TxDOT must protect its data assets from unauthorized and unintended use when the information is being used, in transit, and at rest. TxDOT uses encryption to maintain the confidentiality, ensure the integrity, and prevent unauthorized disclosure of its information.

Digital Signatures - establishes how TxDOT manages the risks of using digital signatures, from their creation through their use, modification, storage, and deletion.

Privacy - discusses how TxDOT safeguards private information which begins when private information is collected and remains in effect through the information's life cycle until disposition. This section describes collecting only the minimum, authorized, necessary information and provides information for curating a tiered, content-based approach.

System and Information Integrity - describes how TxDOT segregates the many functions of information systems to maintain their quality and integrity. As part of its Information Protection Policy, this section requires the separation of systems based on functionality and grants access to a select group of authorized individuals.

Investment Protection

Investment Protection Policy - safeguards the investment in its infrastructure through a robust and rigorous risk management program that allows business programs to optimize their technology-based processes. The intent of the policy is to have safe, reliable, and optimized infrastructure available to authorized users.

Risk Management - establishes how TxDOT protects its investment in information assets through a methodical approach to identify, assess, and reduce risks. It describes the minimum protocol and responsibilities that must be in place to effectively respond to risks and monitor progress.

Physical and Personnel Protection - establishes how TxDOT protects those who work with its information resources as part of its Investment Protection Policy. The effort includes adhering to the policies published in the Agency's State Security Policy Manual and the safety controls established in the Occupational Safety Manual.

Asset Management Protection - establishes how TxDOT manages its information resources assets as part of its Investment Protection policy, and describes the minimum protocols and responsibilities that must be in place to effectively categorize, inventory, maintain, and decommission both physical (tangible) assets such as hardware, physical documents, facilities, etc. and non-physical (intangible) such as intellectual property, digital records, digital connections, virtual machines, etc.

Business Continuity

Business Continuity Policy – addresses creating, testing, and maintaining a system of high-level implementation plans for restoring critical information systems to the latest documented functionality. The intent is to ensure that TxDOT can resume its services after a natural or man-made incident prohibits the Agency from accessing its virtual or physical information resources.

Change Management - establishes how TxDOT uses configuration, change, and patch management processes as part of its Business Continuity policy and describes the minimum standards to effectively support continued business functions when normal operations have been compromised.

Contingency Planning - establishes how TxDOT uses interim measures to recover information resources after a disruption. It describes the minimum standards that must be in place to effectively create a plan for how to respond if routine business operations are suspended.

Incident Response - establishes how TxDOT maintains an Incident Response Plan in order to properly respond to, document, and track incidents. The Incident Response Plan provides a high-level approach for TxDOT's response when information security policies are breached.

Disaster Recovery - TxDOT must plan how to recover and support the continuity of services if a disruption denies access to a primary operations facility. The sole objective of this plan is to re-deploy affected services at a designated alternate site.

5.3 Recommendations

On May 14, 2020, TxDOT was subjected to a ransomware event. Through swift action, and applying the policies and procedures detailed in the "Information Security Policy Manual", TxDOT was able to stop the ransomware event and limit its impact on the information technology systems. TxDOT was quick to act to investigate, analyze and remediate the situation. This event caused temporary interruptions on the agency network as well as business and traffic applications.

The attack affected many TxDOT servers and workstations resulting in total shutdown of TMC operations across the state (with exception of Houston TranStar) for several weeks. District TMCs had to be brought back online one at a time using a "clean" network that was isolated from the internet and all other TxDOT networks. The network included sterile laptops for the operators and Lonestar™ servers that had not been infected or were cleaned after being infected. The most serious damage was to several district database servers that were infected and had to be completely rebuilt using backup databases for Lonestar™. This resulted in some loss of data for districts including Fort Worth and El Paso. Before the attack, TxDOT had some security policies/measures in place including:

- Monthly security patches for TRF and district servers (Lonestar™ servers, database server);
- Citrix accounts for contractors to remote into servers; and
- No sharing passwords policy.

After the attack, TxDOT took additional steps to prevent this from happening again including: 2-factor password validation for all users; and mandatory security training for all employees and contractors who have TxDOT accounts and access to TxDOT servers and workstations.

One of the recommendations included in the TxDOT Statewide TSMO Strategic Plan is for vulnerability analyses to be conducted on a regular basis to provide life cycle protection of critical infrastructure from every type of risk: deliberate, accidental and natural. The vulnerability analyses should consider cyber, wireless and physical domains — identifying vulnerabilities and weaknesses within each domain, focusing on gaps and seams, and aligning critical processes with the critical business technologies to ensure business continuity through improved resilience, preparedness, detection and response.

In accordance with the "Information Security Policy Manual", TxDOT conducts vulnerability assessments on a quarterly rotation for all information resources deployed on its network. The purpose of the quarterly rotation is to ensure all assets are assessed for vulnerabilities on a yearly basis. The assessments are conducted specifically to identify, analyze, and report flaws on the network; in application configurations that are either on or off the network; and in the source code for web applications and services, databases, software, and mobile applications. TxDOT conducts these evaluations within a centrally-managed vulnerability assessment system. It is recommended that the vulnerability assessment system be revisited to address the lessons learned from this recent ransomware event.

6. Performance Management

Performance measures provide TxDOT Leadership with the information they need to support policy and priority decisions. The goal is to apply performance measures to optimize decisions, enhance efficiency, and accelerate results. Performance measures are a critical component of TSMO as they are used to drive continuous improvement in TxDOT's operational efficiency, business processes, organization and workforce, leveraging systems and technology, and collaborating with stakeholder partners. Specifically, performance measures are used to:

- Set goals and standards;
- Detect and correct problems;
- Manage, describe, and improve processes; and
- Document accomplishments.

TxDOT uses Tableau to generate reports from an Amazon Web Services (AWS) data lake which is populated with historical Lonestar™ data and data from other third-party applications. TxDOT started tracking the following three performance metrics on a monthly basis for the six metro districts during 2018 (as previously described in Section 3.3 "Tableau"):

- TMS Asset Uptime;
- Average Incident Clearance Time; and
- Level of Travel Time Reliability.

During 2019, the coastal districts were added as these TMS devices are used to provide information along the evacuation corridors during Hurricane season. It is recommended that these performance measures be rolled out to the remaining districts and "TMS Asset Uptime" consider metrics that account for a more complete complement of systems and technologies including:

- CCTV cameras, vehicle detectors, dynamic message signs (already being measured);
- Communications;
- Lonestar™ ATMS software; and
- IT network systems infrastructure.

The next generation of performance metrics, as they relate to Technology Solutions, is anticipated to focus on developing Artificial Intelligence and Machine Learning applying deep learning predictive tools to be more proactive in managing system and operational performance. This is anticipated to be an iterative process applying lessons learned along the way.

7. Mobility Strategies

Technology solutions described in this report may be integrated as part of mobility strategies to support TSMO goals. Three examples of such mobility strategies include incident management, data analytics, and intelligent work zones.

7.1 Traffic Incident Management

Traffic Incident Management (TIM) is a planned and coordinated program process to detect, respond to, and remove traffic incidents and restore traffic capacity as safely and quickly as possible. On the average, every one-minute of traffic lane closure results in four minutes of traffic delays and queueing (Reference 4). For example, if a traffic lane is closed for 30 minutes, a two-hour delay may be anticipated. Similarly, for every one-minute that an incident remains uncleared, the probability of a secondary crash increases by 2.8% (Reference 5). The quicker the vehicle occupants involved in the crash can receive medical attention by the first responders, their chances of survival significantly improves. Technology solutions play an important role in providing the necessary systems to improve incident detection, response, and clearance times. Such systems include the following:

- **Computer-Aided Dispatch** - Computer-aided dispatch (CAD) is a method of dispatching emergency responders by either sending messages to the responder via a mobile data terminal and/or used to store and retrieve data (i.e., radio logs, field interviews, schedules). Police dispatchers are able to view and understand the status of all units being dispatched. CAD systems consist of several modules that provide services at multiple levels in a dispatch center and in the field of public safety. These services include call input, call dispatching, call status maintenance, event notes, field unit status and tracking, and call resolution and disposition. CAD integration with the Lonestar™ ATMS software would provide a valuable incident detection resource in identifying and verifying incidents.
- **Video Sharing** – Once an incident is detected and verified, TMC operations staff typically pan, tilt, and zoom CCTV cameras to the scene of the incident to determine the extent of impacts (e.g., lane or road closure, hazardous material spill, fatalities, injuries) and resources needed to respond. Video sharing with neighboring districts and affected municipalities can provide broader coverage of the incident impact area, thereby enabling TMC operations staff to deploy the appropriate resources to respond to the primary event while minimizing the potential for excessive queueing and secondary crashes. The Claris system, initiated in the Dallas-Fort Worth region, is being expanded to other areas of the state providing a valuable online website video sharing system for TMC operators and incident responders to use in responding to events.
- **Diversion Routes** – Diversion routes provide an alternate to a primary route if an event causes either a significant or total roadway capacity reduction. These events may include a traffic incident, natural disaster, or emergency rendering a roadway facility impassable. Diverting traffic to a parallel roadway in a carefully planned alternate route plan provides an effective, temporary response to facilitating increased mobility and improved travel time reliability in the corridor. Alternate routes may accommodate local and/or regional traffic. A local alternate route involves diverting primary route traffic a short distance, typically from one point

(e.g., interchange or major intersection) to the next downstream point using a roadway located adjacent to the primary route. Technology solutions and enhancements referenced in this report (e.g., Lonestar™ ATMS software, traffic network monitoring systems) would improve the management capabilities of TMC operations staff and incident responders in the field to manage the corridor more efficiently, thereby minimizing the potential for extensive delays, queueing, and secondary crashes.

Technology solutions also enable TxDOT and incident responders to apply performance measures to monitor, track, and report how well incident management is being performed. Figure 7 illustrates the timeline of a typical incident (Reference 6).

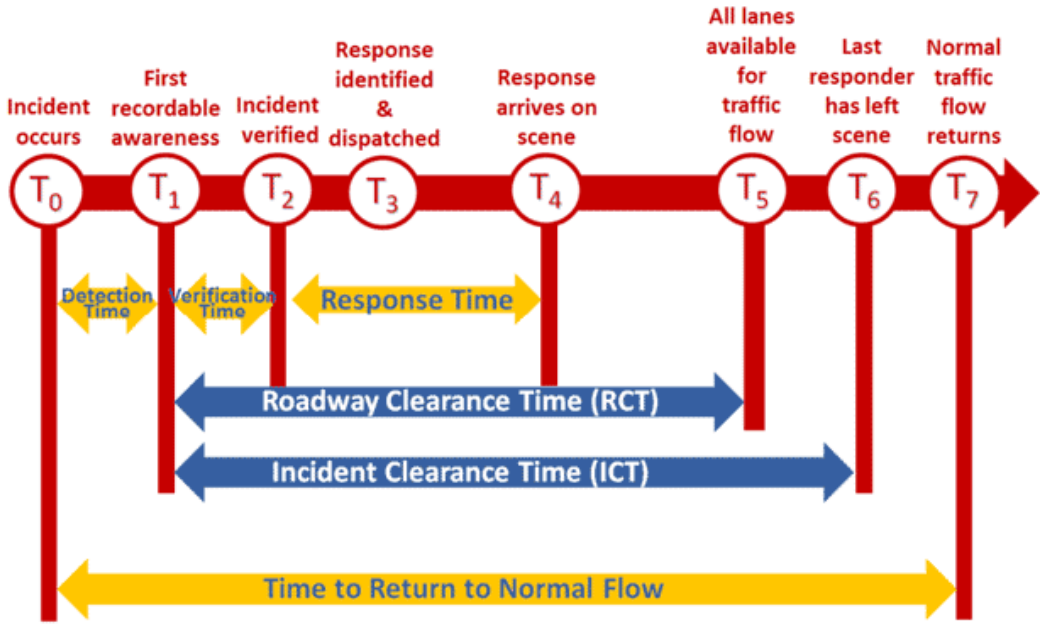


Figure 7: Traffic Incident Timeline (FHWA)

TxDOT may consider adapting Lonestar™ ATMS software and Tableau dashboards to provide this granular level of detail with the goal of minimizing each of the seven timeframes that comprise a typical incident. This higher level of detail would be valuable in conducting "After Action Reviews" of major incidents (or planned special events) to establish lessons learned to apply on future similar events.

7.2 Data Analytics

Data analytics is the science of analyzing raw data in order to make conclusions about that information to optimize an organization's performance. The technology solutions referenced in this report provide a strong foundation in applying data analytics to support TSMO goals such as:

- **Situational Awareness** – Situational awareness is an important component of TSMO in providing a real-time assessment of the transportation system in terms of active incidents, bottlenecks, and assets. This will enable operations and maintenance staff to be more proactive in addressing issues before they become a

problem. The combination of real-time information provided by Lonestar™ ATMS software and Traffic Network Monitoring tools will support this function.

- **Decision Support Systems** - One of the TSMO strategies presented in the TxDOT Statewide TSMO Strategic Plan Update (Reference 7) is "develop Artificial Intelligence (AI) and Machine Learning tools to apply decision support systems to assist in making more informed decisions regarding traffic, safety, incident, emergency, and asset management." These systems should be highly automated to enable the end-users to quickly select the optimum plan based on configurable performance measures. For example, AI/Machine Learning applications may be developed for Incident Management. These systems can be used to develop and archive incident management plans that have been effective for similar incidents in the past while also taking advantage of predictive models. Development of incident management plans should include input by local and regional traffic incident management team members as a result of post-incident analyses. The components of incident management plans may include a library of signal timing plans for diversion routes; automated activation of dynamic message signs; and route guidance for first responders to reach the incident.
- **Performance Management** – Performance management is the cornerstone of TSMO in driving continuous operational improvements. It is recommended that performance measures be measured, tracked and reported in a past, present, and future mode. This will enable TxDOT staff to apply data analytics in measuring the effectiveness of TSMO strategies that have been implemented; provide real-time assessment of transportation systems; and provide predictive capabilities to stay ahead of congestion rather than reacting to it. Figure 9 illustrates how the Florida DOT (District Four, Fort Lauderdale) TMC posts performance measures on the video wall to improve situational real-time awareness.

Figure 8: Florida DOT, District Four TMC Video Wall (Performance Measures)

The above TMC video wall provides real-time performance metrics including the number of active incidents occurring in each of the five counties; the number of emergency generators currently in use; the average incident clearance time, year to date; the number of ITS devices that are currently unavailable; whether there are cuts in the fiber-optic communications network; status of reversible operations along the I-595 express lanes; travel time reliability measures; signal phasing and timing data at critical intersections; and a display of travel speeds by lane and by segment for both general purpose and express lanes.

7.3 *Smart Work Zones*

TxDOT has taken a lead role in the development and implementation of Smart Work Zones. These systems are intended to better inform motorists, encourage them to take alternate routes, reduce their frustrations, reduce freeway congestion, and enhance safety for motorists and workers. Figure 9 below illustrates the various monitoring functions of a smart work zone.

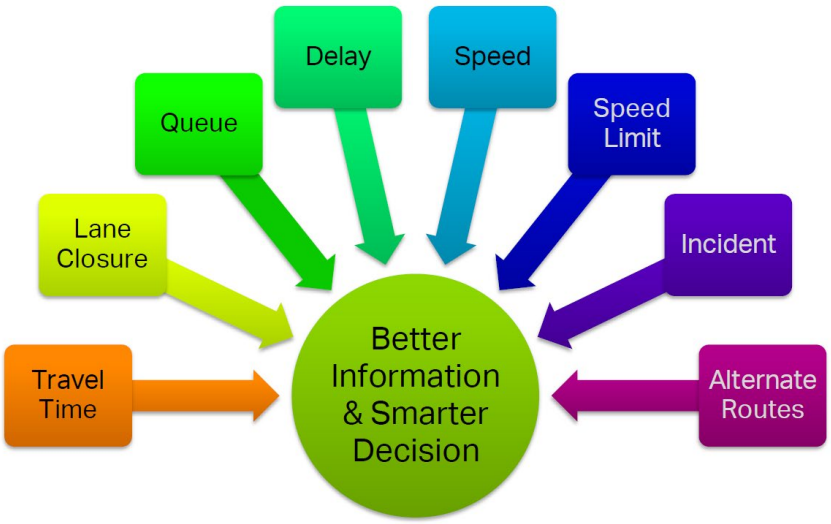


Figure 9: Smart Work Zone

The technology solutions referenced in this report may support the enhancements and effectiveness of smart work zones in achieving TSMO goals through the following strategies:

- **Operational Dashboard** – An operational dashboard provides a centralized place to integrate data from multiple sources such as the smart work zone devices, Lonestar™ ATMS software, TMCs, construction information provided by contractors, municipalities, etc. (Reference 8). Live connection between the ATMS and smart work zone devices (updated every minute) will provide real-time data for live reporting and monitoring of work zone operations and incident response; real-time data to establish performance metrics for work zones; archived data for data analytics to provide detailed analysis and informed decisions (e.g., lane closures, alternate routes, trip planning); archived data to evaluate performance metrics of construction constructors; and comprehensive data collection (e.g., traffic volumes, densities, speeds, incidents, queues, ITS device condition).
- **Worker Safety** – Smart Work Zones should constantly monitor the protected work area using CCTV cameras or radar. If a vehicle encroaches into the work area, the system should alert all workers using a horn and/or on-person alarm system, so they are aware of the potential danger.

- **Connected Vehicle** – Connected vehicle applications will enable communication between a vehicle approaching the smart work zone and ITS infrastructure components. It will also enable vehicle-to-vehicle communication as higher penetration rates of connected vehicles are achieved. Connected vehicle upgrades to smart work zones will require additional edge computing capabilities in sharing information in real-time rather than being subjected to latency in communicating with TMCs. Connected vehicles will be able to acquire real-time information regarding queues, speeds, construction equipment merging into traffic, travel times, incidents, lane closures, and over-height restrictions.

Performance measures will allow TxDOT to monitor work zone operations and its effects on roadway conditions with incentives or disincentives in the contract. For example, a contractor may receive a financial bonus each day they are off the roadway before 6:00 am, prior to morning peak hour commute traffic. Alternatively, a contractor may receive a financial disincentive each day they are not off the roadway by a certain time (Reference 9). Contractor incentives and disincentives have also been applied in other states for maintaining a targeted travel speed (e.g., 45 mph) during certain times of the day. ITS tools support the accuracy of these measurements to ensure fair treatment of contractors and DOTs.

8. Summary

In summary, technology plays an important role in the successful implementation of TSMO strategies to improve operational effectiveness. As a precursor to emerging technologies, the existing ITS infrastructure needs to be expanded and modernized to provide reliable communications and data management systems. This is particularly important as connected vehicles will generate a tremendous amount of real time data that will need to be managed. The recommendations presented in this report should be shared with TxDOT Leadership including, but not limited to, the following:

- Strategy & Innovation Division
- Information Technology Division
- Traffic Safety Division
- Emerging Technology Task Force
- Technology Innovation Alliance
- Autonomy Institute
- Transportation Research Centers

This collaboration would cast a wide net of stakeholders in identifying new technologies to address TSMO goals. It may also provide an opportunity to bring a higher level of collaboration between TxDOT, technology vendors, consultants, contractors, Original Equipment Manufacturers (OEM), research companies, data providers, and others in developing public-private partnerships. For example, public-private partnerships may be formed with telecommunications companies by providing them access to TxDOT right-of-way in exchange for providing TxDOT fiber. Another example is having a private company (or OEM) provide data (and possibly data analytics) hosted on their data platforms (cloud) and share the data that TxDOT needs in exchange for payment as a service. These and other partnerships should be explored, with due diligence conducted considering risks and value to the Department, to enable TxDOT and the public to use technology in making more informed data-driven decisions.

References

1. TxDOT, “Network Monitoring and Management”, presentation by NTT Data / Skyline Technology Solutions, August 2020.

2. TxDOT, Information Technology Website.

3. TxDOT, “Information Security Policy Manual”, November 2017.

4. FHWA Traffic Incident Management Handbook; https://ops.fhwa.dot.gov/eto_tim_pse/about/tim.htm

5. Karlaftis, Latoski & Sinha Richards, "ITS Impacts on Safety and Traffic Management: An Investigation of Secondary Crash Causes," ITS Journal,1999, Vol. 5.

6. USDOT, FHWA Office of Operations, “Traffic Incident Management Gap Analysis Primer”, May 13, 2020.

7. TxDOT, “Statewide TSMO Strategic Plan”, prepared by AECOM, May 2020.

8. TxDOT, “Smart Work Zones, from Planning to Implementation”, prepared by AECOM, February 27, 2018.

9. Washington State DOT, “Work Zone Intelligent Transportation System”, prepared by the TSMO Division, 2020.