

# **EMERGING PRACTICES FOR COMMUNICATIONS INFRASTRUCTURE**

## **FINAL REPORT**

---

**October 9, 2020**

**ENTERPRISE TRANSPORTATION POOLED  
FUND STUDY TPF-5(359)**

**Prepared by:  
Athey Creek Consultants**



**Technical Report Documentation Page**

1. Report No. ENT-2020-6	2. Government Accession No.	3. Recipients Catalog No.	
4. Title and Subtitle Emerging Practices for Communications Infrastructure		5. Report Date October 9, 2020	
		6. Performing Organization Code	
7. Author(s) Linda Preisen and Tina Roelofs		8. Performing Organization Report No.	
9. Performing Organization Name and Address Athey Creek Consultants 2097 County Road D, Suite C-100 Maplewood, MN 55109		10. Project/Task/Work Unit No.	
		11. Contract (C) or Grant (G) No. 2019-0045	
12. Sponsoring Organization Name and Address ENTERPRISE Pooled Fund Study TPF-5(359) Michigan DOT (Administering State) PO Box 30050 Lansing, MI 48909		13. Type of Report and Period Covered Final Report	
		14. Sponsoring Agency Code	
15. Supplementary Notes Final Report available at: <a href="http://enterprise.prog.org/Projects/2020/ENT-Emerg-Pracs-Communs-Infra-Final-Report.pdf">http://enterprise.prog.org/Projects/2020/ENT-Emerg-Pracs-Communs-Infra-Final-Report.pdf</a>			
16. Abstract Transportation agencies that operate Intelligent Transportation System (ITS) field devices and systems continually adapt their communications infrastructure to meet emerging needs, improve efficiency, increase coverage, and improve operations. As agencies begin to implement connected and automated vehicle (CAV) systems, they are seeking backbone communications options that can serve multiple purposes. This research utilized a “customer-centric” (agency-focused) approach to document emerging practices for ITS communications infrastructure. This report explores agencies’ long-distance data communications needs and options for related infrastructure, with focus on emerging technologies, including: considerations for selecting communications infrastructure; costs, benefits, and performance; options for ownership, leasing, and security; and developments in edge computing and cloud computing. The report also documents long-term management practices for long-distance data communications infrastructure assets including broadband access to agency owned right-of-way and sharing options; fiber tracking; managing leases and licenses; physical security of ITS devices and communications infrastructure; and cybersecurity practices.			
17. Key Words communication infrastructure, wireless, fiber, cellular, backhaul, 5G, intelligent transportation systems, ITS, field devices		18. Distribution Statement No restrictions	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 88	22. Price

## Acknowledgements

---

This *Emerging Practices for Communications Infrastructure* report was prepared for the ENTERPRISE Transportation Pooled Fund TPF-5(359) program (<http://enterprise.prog.org/>). The primary purpose of ENTERPRISE is to use the pooled resources of its members from North America and the United States federal government to develop, evaluate, and deploy Intelligent Transportation Systems (ITS).

The cover page image was provided courtesy of the Minnesota Department of Transportation.

### Project Champions

Kevin Price, Illinois Department of Transportation; Susan Boot, Ontario Ministry of Transportation; and Jim Tamarelli, Michigan Department of Transportation were the ENTERPRISE Project Champions for this effort. The Project Champions serve as the overall leads for the project.

### ENTERPRISE Members

The ENTERPRISE Board consists of a representative from each of the following member entities.

- Illinois Department of Transportation
- Iowa Department of Transportation
- Kansas Department of Transportation
- Michigan Department of Transportation
- Ontario Ministry of Transportation
- Minnesota Department of Transportation
- Pennsylvania Department of Transportation
- Texas Department of Transportation
- Wisconsin Department of Transportation

### Input from Agencies and Cellular Service Carriers

ENTERPRISE would like to acknowledge and thank the following entities who participated in phone interviews, completed a question guide, or provided other input for this project:

#### Transportation Agencies:

- California Department of Transportation
- Florida Department of Transportation
- Georgia Department of Transportation
- Michigan Department of Transportation
- Minnesota Department of Transportation
- New Hampshire Department of Transportation
- North Dakota Department of Transportation
- Ontario Ministry of Transportation
- Utah Department of Transportation
- Wisconsin Department of Transportation

#### Cellular Service Carriers:

- AT&T
- Verizon

## Acronyms

---

<b>ACL</b> – Access Control Lists	<b>MEC</b> – Multi-access Edge Computing
<b>ADOT</b> – Arizona DOT	<b>mmWave</b> – millimeter waves
<b>ARMER</b> – Allied Radio Matrix for Emergency Response	<b>MnDOT</b> – Minnesota Department of Transportation
<b>ATR</b> – Automatic Traffic Recorder	<b>MPLS</b> – Multiprotocol Label Switching
<b>ATMS</b> – Advanced Traffic Management Software	<b>MTO</b> – Ontario Ministry of Transportation
<b>BSM</b> – Basic Safety Messages	<b>NCHRP</b> – National Cooperative Highway Research Program
<b>Caltrans</b> – California Department of Transportation	<b>NDDOT</b> – North Dakota Department of Transportation
<b>CAV</b> – Connected and Automated Vehicle	<b>NHDOT</b> – New Hampshire Department of Transportation
<b>CCTV</b> – Closed-Circuit Television	<b>NMS</b> – Network Management System
<b>CIS</b> – Center for Internet Security	<b>NOAA</b> – National Oceanic and Atmospheric Administration
<b>CRR</b> – Cyber Resilience Review	<b>NOCoE</b> – National Operations Center of Excellence
<b>CV</b> – Connected Vehicle	<b>NSA</b> – U.S. National Security Agency
<b>DAS</b> – Distributed Antenna System	<b>NTIA</b> – National Telecommunications and Information Administration
<b>DeIDOT</b> – Delaware DOT	<b>P3</b> – Public-Private Partnership
<b>DHS</b> – U.S. Department of Homeland Security	<b>ROW</b> – Right-of-way
<b>DMS</b> – Dynamic Message Sign	<b>RSU</b> – Roadside unit
<b>DMZ</b> – Demilitarized Zone	<b>RWIS</b> – Road Weather Information Systems
<b>DSRC</b> – Dedicated Short-range Radio Communications	<b>SCMS</b> – Security Credential Management System
<b>EDCM</b> – Event Driven Configurable Messaging	<b>SPaT</b> – Signal Phase and Timing
<b>FCC</b> – Federal Communications Commission	<b>SSL</b> – Secure Sockets Layer
<b>FDOT</b> – Florida Department of Transportation	<b>SWF</b> – Small Wireless Facility
<b>FirstNet</b> – First Responder Network Authority	<b>TMC</b> – Traffic Management Center / Transportation Management Center
<b>FTM</b> – Field Traffic Master	<b>TRB</b> – Transportation Research Board
<b>GDOT</b> – Georgia Department of Transportation	<b>TSMO / TSM&amp;O</b> – Transportation Systems Management and Operations
<b>GIS</b> – Geographic Information System	<b>TxDOT</b> – Texas DOT
<b>GOES</b> – Geostationary Operational Environmental Satellite	<b>UDOT</b> – Utah Department of Transportation
<b>HAR</b> – Highway Advisory Radio	<b>USDOT</b> – U.S. Department of Transportation
<b>IDOT</b> – Illinois DOT	<b>V2I</b> – Vehicle to Infrastructure
<b>IoT</b> – Internet of Things	<b>V2X</b> – Vehicle to everything
<b>IT</b> – Information Technology	<b>VPN</b> – Virtual Private Network
<b>ITS</b> – Intelligent Transportation Systems	<b>WIM</b> – Weigh-in-motion
<b>ITSFM</b> – ITS Facilities Management	<b>WisDOT</b> – Wisconsin Department of Transportation
<b>LPWA</b> – Low Power Wide Area	
<b>LPWAN</b> – Low Power Wide Area Network	
<b>LTE</b> – Cellular	
<b>LTE-M</b> – Cellular service using LPWAN	
<b>MAC</b> – Media Access Control	
<b>MAP</b> – Roadway geometry data	
<b>MDOT</b> – Michigan Department of Transportation	

## Table of Contents

<b>1.0</b>	<b>Introduction</b>	<b>1</b>
<b>2.0</b>	<b>Project Approach</b>	<b>3</b>
2.1	Transportation Agencies	3
2.2	Cellular Service Carriers	4
<b>3.0</b>	<b>Needs for Long-Distance Data Communications to Field Devices</b>	<b>5</b>
3.1	Traditional Long-Distance Data Communication Needs	5
3.2	Emerging Long-Distance Data Communications Needs	6
3.3	Summary of Long-Distance Data Communications Needs	8
<b>4.0</b>	<b>Current and Emerging Use of Cellular for Communication to Field Devices</b>	<b>9</b>
4.1	Agency Use of Cellular Service	9
4.2	Emerging Cellular Services	10
4.2.1	5G Cellular	10
4.2.2	First Responder Network Authority (FirstNet)	12
4.2.3	Low-Power Wide-Area Networks (LPWAN)	14
<b>5.0</b>	<b>Selecting Communications Infrastructure</b>	<b>15</b>
5.1	Selection Considerations	15
5.2	Tradeoffs with Ownership versus Leasing or Procuring Services	16
5.3	Edge Computing, Cloud Computing, and Exception Communications	17
5.4	Connected Vehicle Backhaul	19
<b>6.0</b>	<b>Long-term Management Practices</b>	<b>22</b>
6.1	Permitting for 5G Small Cell Deployments in Right-of-Way	22
6.2	Right-of-Way Access, Co-Location, and Resource Sharing	26
6.2.1	Access to Broadband Facilities	26
6.2.2	Co-location on DOT-owned Towers	26
6.2.3	Fiber Sharing, Resource Trading, and Public-Private Partnerships	27
6.3	Fiber Tracking	29
6.4	Managing Licenses and Agreements	32
6.4.1	FCC Licenses	32
6.4.2	Co-location Agreements	32
<b>7.0</b>	<b>Security</b>	<b>33</b>
7.1	Physical Security – Agency Practices	33
7.1.1	Monitoring Field Devices and Communications Networks	33
7.1.2	Field Boxes, Shelters and Cabinets	33
7.1.3	Towers and Buildings	34
7.2	Cybersecurity – Agency Practices and Cellular Service Protections	35
7.3.1	General Cybersecurity Practices	35
7.3.2	Connected Vehicle Infrastructure and Data Security	36
7.3.3	Cellular Service Cybersecurity Protections	36
7.2	Cybersecurity Resources	37
7.2.1	Transportation Management Center Information Technology Security	38
7.2.2	Cybersecurity of Traffic Management Systems	43
<b>8.0</b>	<b>Summary</b>	<b>45</b>
	<b>Appendix A: Input from Transportation Agencies</b>	<b>A-1</b>
	<b>Appendix B: Input from Cellular Service Carriers</b>	<b>B-1</b>
	<b>References</b>	<b>Ref-1</b>

## 1.0 Introduction

---

Transportation agencies that operate Intelligent Transportation System (ITS) field devices and systems continually adapt their communications infrastructure to meet emerging needs, improve efficiency, increase coverage, and improve operations. As agencies begin to implement connected and automated vehicle (CAV) systems, they are seeking backbone communications options that can serve multiple purposes. As such, agencies need to understand various aspects of emerging communications infrastructure options, including capabilities of emerging technologies as well as management practices in terms of planning, performance, and security. There is also a need to understand how more traditional options (e.g. fiber) compare to newer technologies (e.g. latest available cellular services), how to plan for these options, and practices for managing the resulting assets.

This project *Emerging Practices for Communications Infrastructure* utilized a “customer-centric” (i.e. agency-focused) approach to document emerging practices for ITS communications infrastructure. The research focused on the following themes:

This project utilized a “customer-centric” approach to document emerging practices for ITS communications infrastructure.

- ***Agencies’ long-distance data communications needs, and how those needs are changing:***
  - On-site data processing and a trend toward “exception” communications (versus continuous communications to devices);
  - Communications for CAV data backhaul, including data exchanges between roadside units and a central location, and transfers of large data sets over long distances; and
  - Potential for wireless communications services to perform similar functions as fiber, with pricing strategies that may support non-continuous communications needs.
- ***Options for long-distance communication infrastructure, with focus on emerging technologies:***
  - Considerations for selecting long-term communications infrastructure;
  - Costs, benefits, and performance;
  - Options for ownership, leasing, and security; and
  - Developments in computing topology (i.e. edge and ubiquitous computing).
- ***Management practices for communications infrastructure assets:***
  - Broadband access to agency owned right-of-way and sharing options;
  - Long-term management practices such as fiber tracking and managing leases or licenses;
  - Physical security of ITS devices and communications infrastructure; and
  - Cybersecurity practices and resources for field devices and traffic management centers.

It is important to note that this project did not conduct a comparison of the available technologies for low latency, short-distance CAV data communications. Rather, it focused on long-distance data communications to support CAV applications in the overall context of how agencies select and manage communications infrastructure.

## **Report Sections:**

This report includes the following sections:

- [2.0 Project Approach](#) – Describes the approach for this research and lists the transportation agencies and cellular service providers that provided input.
- [3.0 Needs for Long-Distance Data Communications to Field Devices](#) – Discusses multiple scenarios for traditional and emerging field device communications needs.
- [4.0 Current and Emerging Use of Cellular for Communication to Field Devices](#) – Presents an overview of agency use of cellular services for long-distance data communications and discusses emerging cellular services such as 5G, FirstNet, and low-power wide-area networks (LPWAN).
- [5.0 Selecting Communications Infrastructure](#) – Provides an overview of factors agencies use to select mechanisms for data communications to field devices and trade-offs with ownership versus leasing or procuring services.
- [6.0 Long-term Management Practices](#) – Presents practices for installing small wireless facilities and other broadband facilities on highway rights-of-way, co-location on agency-owned structures, resource trading, public-private partnerships, fiber sharing, fiber tracking, and managing licenses and agreements.
- [7.0 Security](#) – Provides agency practices for physical security and cybersecurity, along with a summary of recent published cybersecurity resources applicable to traffic and ITS operations.
- [8.0 Summary](#) – Presents highlights of project findings.

## 2.0 Project Approach

---

This project first documented transportation agencies' long-distance data communications needs and how those needs are changing. This step was completed to refine key research questions and identify areas of inquiry for interviews with agencies and input from cellular service carriers.

The project then gathered information via the following mechanisms, to identify current practices and emerging trends for long-distance data communications for field devices and associated long-term management practices:

- **Input from transportation agencies** – Representatives from ten (10) transportation agencies participated via phone interviews or provided written input;
- **Input from cellular service carriers** – Representatives from two commercial cellular service carriers provided information via a phone interview or provided links to company literature; and
- **Online resources and published literature** – Information from online resources and published literature was referenced to supplement input from agencies and cellular carriers.

Upon review of the information gathered, observations and examples were compiled around key topic areas, including current and emerging use of cellular for data communication to field devices, selection considerations, right-of-way access and long-term management practices (right-of way access for 5G small cell deployments and other types of communications facilities, sharing communications infrastructure, tracking fiber, managing licenses and leases), physical security of field assets, and cybersecurity.

### 2.1 Transportation Agencies

Representatives from 10 transportation agencies (nine U.S. state agencies and one Canadian provincial agency) provided input for this research via phone interviews or by completing a question guide:

- California Department of Transportation (Caltrans)
- Florida Department of Transportation (FDOT)
- Georgia Department of Transportation (GDOT)
- Michigan Department of Transportation (MDOT)
- Minnesota Department of Transportation (MnDOT)
- New Hampshire Department of Transportation (NH DOT)
- North Dakota Department of Transportation (NDDOT)
- Ontario Ministry of Transportation (MTO)
- Utah Department of Transportation (UDOT)
- Wisconsin Department of Transportation (WisDOT)

Input provided by transportation agencies through interviews or a completed question guide included the following areas of inquiry and was supplemented by reviewing online resources and published literature:



- Current and emerging use of cellular service for data communications to field devices
- Selecting communications infrastructure
  - Costs and performance
  - Tradeoffs with owned assets vs. leased services
  - Trend toward “exception” communications
  - Edge and cloud computing solutions
  - Current and future CAV backhaul needs
- Long-term management practices
  - Right-of-way access
  - Sharing options and agreements
  - Tracking (fiber tracking, managing leases or licenses)
  - Physical security and cybersecurity

**Input from Agencies**

- Current and emerging use of cellular
- Selecting communications infrastructure
- Long-term management practices

Full summaries of input gathered from each agency can be found in Appendix A.

In addition to formal participation by the agencies listed above, practices from Illinois DOT (IDOT), Texas DOT (TxDOT), and Delaware DOT (DeIDOT) have been documented in this report through review of online resources and/or from information received via email.

## 2.2 Cellular Service Carriers

Representatives from two commercial cellular service carriers provided information for this research. Participation by cellular service carrier varied in terms of the input provided and applicability to long-distance data communications to ITS field devices. The following cellular service carriers that provided input are listed below, along with how they participated.

- AT&T – Participated in a phone interview, responding to the project’s question guide
- Verizon – Submitted company literature related to services applicable to transportation agencies

Input requested from cellular service carriers included the following areas of inquiry and was supplemented by reviewing online resources and company literature:

- Cellular services offered (e.g. 3G, 4G, 4G LTE, 5G)
- Rate plans and pricing structures
- Alternatives to traditional service agreements (e.g. public-private partnerships, ownership, or leasing)
- Cybersecurity protection assurances
- Where and to what degree 5G services are available (e.g. test sites, pilots) and expansion plans

**Input Requested from Cellular Carriers**

- Cellular services offered
- Rate plans and pricing
- Alternatives to traditional service agreements
- Cybersecurity
- Extent of 5G deployments

The full summaries of input gathered from cellular service carriers can be found in Appendix B.

## 3.0 Needs for Long-Distance Data Communications to Field Devices

This section summarizes transportation agencies’ long-distance data communications infrastructure needs and how those needs are changing. This step was completed to refine key research questions and identify areas of inquiry for agency and private sector interviews. The scenarios detailed in this section are used to describe long-distance data communications needs and are grouped into “traditional” and “emerging” long-distance data communications needs. Describing these scenarios helped to identify differences between traditional and emerging needs that play a role in how transportation agencies may be modifying their communications infrastructure and plan for future needs.

### 3.1 Traditional Long-Distance Data Communication Needs

These scenarios describe long-distance data communications needs that primarily support more conventional ITS field devices, such as dynamic message sign (DMS), road weather information systems (RWIS), and traffic cameras. These scenarios rely on extensive long-distance communications infrastructure networks to continually (or nearly continually) communicate data from field devices to/from a central location for data collection, data storage, or device control.

- **Scenario 1 - Continuous Long-Distance Data Communications (High Bandwidth):**  
Communications to/from field devices that transfer large volumes of data requiring high bandwidth long-distance communications capabilities.
- **Scenario 2 – Continuous Long-Distance Data Communications (Low Bandwidth):**  
Communications to/from field devices that transfer lower volumes of data requiring lower bandwidth long-distance communications.

Tables 1 and 2 show characteristics, examples, and long-distance data communications needs for Scenarios 1 and 2, respectively.

**Table 1: Scenario 1 - Continuous Long-Distance Data Communications (High Bandwidth)**

<b>Characteristics</b>	<ul style="list-style-type: none"> <li>• Continuous communications back to a central location</li> <li>• Relies on local device-to-device communications in the field provided by separate communications mechanisms</li> <li>• Large volumes of data</li> </ul>
<b>Examples</b>	<ul style="list-style-type: none"> <li>• Traffic cameras with video feeds to a Traffic Management Center (TMC)</li> <li>• Traffic detection field devices providing data to centrally located TMC systems</li> </ul>
<b>Long-distance Data Communications Needs</b>	<ul style="list-style-type: none"> <li>• Frequency ==&gt; Continuous</li> <li>• Latency (speed of data transfer) ==&gt; Low to Moderate</li> <li>• Bandwidth (volume of data) ==&gt; High</li> <li>• Security ==&gt; Moderate</li> <li>• Reliability ==&gt; Moderate to High</li> </ul>

**Table 2: Scenario 2 - Continuous Long-Distance Data Communications (Low Bandwidth)**

<b>Characteristics</b>	<ul style="list-style-type: none"> <li>Nearly continuous (e.g. periodic, pre-determined intervals) communications back to a central location</li> <li>Relies on local device-to-device communications in the field provided by separate communications mechanisms</li> <li>Small volumes of data</li> </ul>
<b>Examples</b>	<ul style="list-style-type: none"> <li>RWIS stations that regularly (e.g. once per hour) report back to a central location</li> <li>DMS in high use locations, to post and modify messages</li> </ul>
<b>Long-distance Data Communications Needs</b>	<ul style="list-style-type: none"> <li>Frequency ==&gt; Nearly Continuous</li> <li>Latency (speed of data transfer) ==&gt; Moderate</li> <li>Bandwidth (volume of data) ==&gt; Low</li> <li>Security ==&gt; Moderate to High</li> <li>Reliability ==&gt; Moderate</li> </ul>

### 3.2 Emerging Long-Distance Data Communications Needs

The first scenario in this category (Scenario 3) describes long-distance data communications needs that indicate a trend toward “exception” communications, with potentially less reliance on communications infrastructure. The second scenario in this category (Scenario 4) describes long-distance data communications needs for the quickly emerging need for centrally located transportation operations systems to communicate with CAV infrastructure systems in the field.

- Scenario 3 – “Exception” Long-Distance Data Communications for Local Field Devices and Systems:** Long-distance data communications to/from field devices that largely operate locally in the field with minimal interaction from a central site. Long-distance communications are by exception only, typically for operators to monitor the status or operational health of field devices, or to send over-ride commands to devices. Data processing in the field can vary from simple field device operations to more complex computations and operations. However, some agencies may wish to move toward simplifying their communications networks by de-centralizing complex data processing functions in order to free up bandwidth for other uses or to re-allocate staff resources that have traditionally been required to manually operate systems from a central location.
- Scenario 4 – Continuous Long-Distance Communications for CAV Data Backhaul:** Long-distance communications to transfer large volumes of data from CAV infrastructure systems in the field back to a central location (i.e. TMC) where the data is processed and to transfer processed data from the central location to the CAV infrastructure systems in the field.

Tables 3 and 4 show characteristics, examples, and long-distance data communications needs for Scenarios 3 and 4, respectively.

**Table 3: Scenario 3 – “Exception” Long-Distance Data Communications for Local Field Devices**

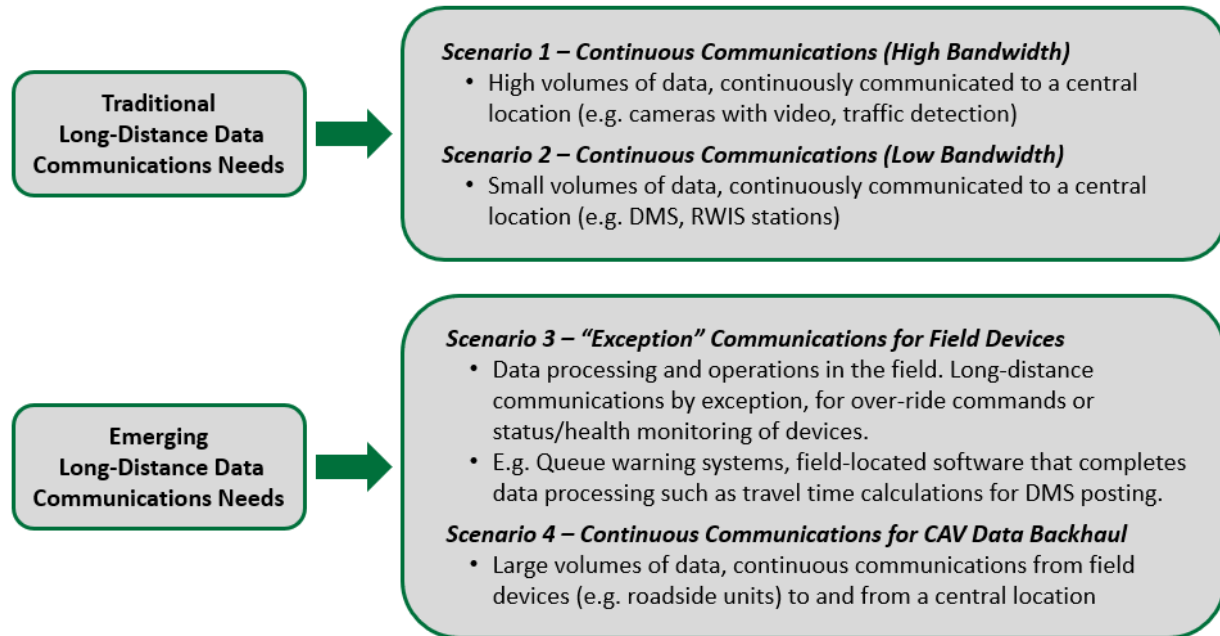
<b>Characteristics</b>	<ul style="list-style-type: none"> <li>• Data processing and operations are automated and occur in the field</li> <li>• Long-distance communications are by “exception,” typically for over-ride commands or for status/health monitoring of devices</li> </ul>
<b>Examples</b>	<ul style="list-style-type: none"> <li>• Low Latency Data Processing in the Field                             <ul style="list-style-type: none"> <li>○ Data processing in the field is essential, due to local low latency requirements for detecting conditions and quickly initiating local device activations and control.</li> <li>○ Examples: smart roadway lighting systems, ITS warning systems (e.g. queue warnings, over-height vehicle warnings, curve warnings)</li> </ul> </li> <li>• Edge Computing in the Field                             <ul style="list-style-type: none"> <li>○ Data processing in the field may not be essential to operations; however, agencies may wish increase use of edge computing for some operational systems.</li> <li>○ An example is advanced traffic management software (ATMS) units located in the field that process traffic detection data, calculate travel times, and automatically post travel times to nearby DMS.</li> </ul> </li> </ul>
<b>Long-distance Data Communications Needs</b>	<ul style="list-style-type: none"> <li>• Frequency ==&gt; “Exception” only</li> <li>• Latency (speed of data transfer) ==&gt; Low</li> <li>• Bandwidth (volume of data) ==&gt; Low</li> <li>• Security ==&gt; Low to Moderate</li> <li>• Reliability ==&gt; Moderate</li> </ul>

**Table 4: Scenario 4 - Continuous Long-distance Communications for CAV Data Backhaul**

<b>Characteristics</b>	<ul style="list-style-type: none"> <li>• Primarily continuous communications from field devices to/from a central location</li> <li>• Could include large volumes of data</li> </ul>
<b>Examples</b>	<ul style="list-style-type: none"> <li>• Agencies may use Event Driven Configurable Messaging (EDCM) to poll CAVs to respond with information such as queues or stopped vehicles, mandating the need for continuous communications</li> <li>• Agencies that capture Basic Safety Messages (BSM) from vehicles may either process these in the field or communicate the raw data back to central locations for processing or storage</li> </ul>
<b>Long-distance Data Communications Needs</b>	<ul style="list-style-type: none"> <li>• Frequency ==&gt; Continuous</li> <li>• Latency (speed of data transfer) ==&gt; Moderate</li> <li>• Bandwidth (volume of data) ==&gt; High</li> <li>• Security ==&gt; Moderate</li> <li>• Reliability ==&gt; Moderate to High</li> </ul>

### 3.3 Summary of Long-Distance Data Communications Needs

Figure 1 provides a visual overview of the four scenarios described above for transportation agencies that fall within traditional or emerging long-distance data communications needs.



**Figure 1: Traditional and Emerging Long-Distance Data Communications Needs**

The trends below outline ways in which long-distance data communications needs may be changing for transportation agencies:

- A potential trend toward increased use of “exception communications” through edge computing or ubiquitous data processing at the location of field devices rather than continuous communications to a central location for data processing.
- A future that may require high bandwidth communications capabilities for CAV backhaul to send large volumes of data to a central location for data processing or data storage.
- Increased options for wireless communications services that could perform functions similar to fiber with pricing strategies that may support non-continuous communications needs.

The following sections of this report provide results from information-gathering from transportation agencies, cellular service providers, online resources, and published literature, to describe current and emerging practices for long-distance data communications to field devices.

## 4.0 Current and Emerging Use of Cellular for Communication to Field Devices

---

This section provides key highlights from the interviews and discusses cellular services for long-distance data communications to transportation field devices, including current agency use of cellular service and emerging technologies and services.

### 4.1 Agency Use of Cellular Service

Transportation agencies use cellular service to support a variety of field device applications. Many agencies reported using cellular where reasonable access to a physical communication connection (e.g. fiber) is not available, or to connect into a fiber line for a hybrid approach. The following provides common uses for cellular field device communications, access to cellular service, cost considerations and rate plans, and general performance.

#### Common Uses for Cellular:

- Cellular service is well-suited for the following:
  - Field devices such as DMS, weather stations, highway advisory radio, traffic signals, weigh-in-motion devices, automated traffic recorders, and ramp meters that do not need continuous communication and can operate using low bandwidth communications.
  - Mobile devices to report road conditions and maintenance needs as needed or required.
  - Temporary ITS applications such as portable traffic cameras or DMS used for work zones, special events, or emergency operations.
- Some agencies may use cellular for high bandwidth devices such as traffic cameras, mainly at locations where fiber is not available.
- **MTO** deploys cellular modems at strategic cabinet locations, as a backup in case a fiber outage occurs, to maintain continuity of operations.

#### Common Uses for Cellular

- Low bandwidth devices (e.g. DMS, weather stations, traffic signals)
- Mobile devices
- Temporary applications

#### Access to Cellular Service:

- Transportation agencies procure services from commercial cellular carriers.
- A few agencies noted that cellular coverage is spotty or non-existent in some rural areas.

#### Cost Considerations and Rate Plans:

- Cellular can be the most economical option (compared to building new infrastructure) for low-bandwidth applications, especially if a fiber connection is not nearby.
- Many agencies have statewide contracts with cellular service carriers, with pre-negotiated rates based on device needs and available services.

- Cellular services often have a monthly fee per device/modem with additional charges based on usage. Unlimited data plans can be procured for high data needs (e.g. video from cameras).
- **MTO** reported that a pre-negotiated plan with a specific vendor to supply modems has helped to control costs.
- **NDDOT** indicated that cellular carriers will typically work with the agency when overages occur due to weather events where usage (e.g. cameras) sharply increases from typical.
- AT&T noted pooled rate plans that include multiple devices with multiple data “buckets” and flexibility for overages when the next available data “bucket” can be accessed.

#### Cellular Performance

- Often meets agency needs where coverage is good and for low-bandwidth devices.
- Performance lags or is insufficient at high use sites (e.g. near a stadium) or at high use periods (e.g. during evacuations) with heavy cellular phone use.

#### Performance:

- The performance of cellular (e.g. reliability, bandwidth) generally meets agencies’ needs for communicating to field devices, especially where cellular coverage is sufficient and lower bandwidth device applications are connected.
- Agencies noted that cellular performance can lag or is insufficient/unreliable at high use sites (e.g. near a stadium during an event) or during high use periods (e.g. during an evacuation) with heavy cellular phone use.

## 4.2 Emerging Cellular Services

The emerging cellular services described in this section include technologies or services that have become available in recent years, are being explored for potential future use, or are emerging options for field device applications. For example, 5G cellular service has gained much attention due to its expected high-speed, low latency data transfer capabilities. The First Responder Network Authority (FirstNet) that is being built out across the U.S. to support dedicated communications for emergency responders and supporting entities offers a new option for agencies to consider for field device communications. Lastly, low-power wide-area networks (LPWAN) can offer lower rate plans for low-bandwidth field device applications.

### 4.2.1 5G Cellular

5G is the fifth generation wireless technology for digital cellular networks that began wide deployment in 2019.<sup>1</sup> 5G operates in three frequency bands that are broadly termed as “high band,” “mid band,” and “low band.” An online article from the *Qualcomm Developer Network* describes 5G frequency ranges as below 1 GHz for low band, 1 GHz to 6 GHz for mid band, and above 24 GHz for millimeter wave (mmWave)

---

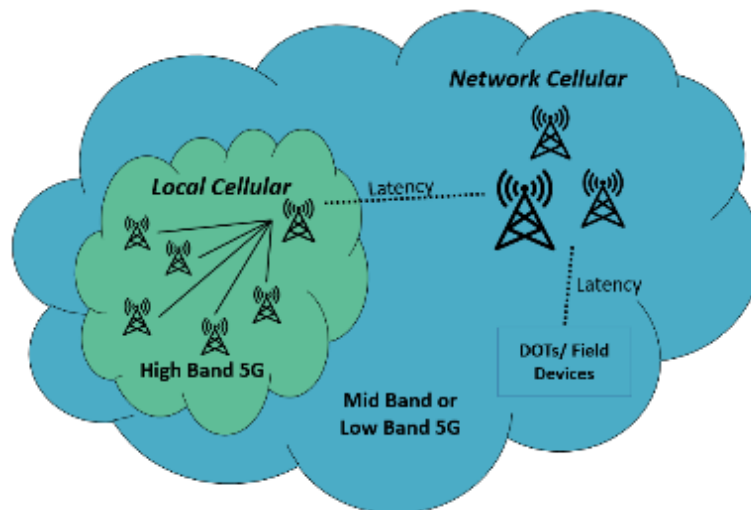
<sup>1</sup> <https://en.wikipedia.org/wiki/5G>

high band.<sup>2</sup> General characteristics and expected uses of 5G vary within these bands as broadly described in Table 5.

**Table 5: Frequency Bands, Characteristics and Expected Uses for 5G**

Frequency Band	Characteristics <sup>3</sup>	Expected Uses
<b>High Band</b>	<ul style="list-style-type: none"> <li>• Uses millimeter waves (mmWave)</li> <li>• Fastest, with speeds often 1–2 Gb/s down</li> <li>• Reach is short, therefore more cells (antennas) are required</li> </ul>	<ul style="list-style-type: none"> <li>• Local cellular, for short-range, point-to-point communications</li> <li>• Could supplement or replace dedicated short-range radio communications (DSRC) for connected vehicle applications</li> </ul>
<b>Mid Band</b>	<ul style="list-style-type: none"> <li>• Most widely deployed</li> <li>• Speeds usually 100–400 Mb/s down</li> <li>• Many areas can be covered by upgrading existing towers, which lowers the cost</li> </ul>	<ul style="list-style-type: none"> <li>• Network cellular, for long-distance data communications</li> <li>• Soon to be more widely available, with better performance than current 4G</li> </ul>
<b>Low Band</b>	<ul style="list-style-type: none"> <li>• Speeds typically less than 100 Mb/s</li> <li>• Similar capacity as advanced 4G</li> <li>• Performance will improve but cannot be significantly greater than 4G in same spectrum</li> </ul>	<ul style="list-style-type: none"> <li>• Network cellular, for long-distance data communications</li> <li>• Similar performance as current 4G</li> </ul>

Figure 2 shows a graphic that depicts “local cellular” (high-band 5G with high speeds, low latency, short-range, point-to-point communications) and “network cellular” which encompasses the mid-and low-band frequencies and communicates data over longer distances with slower speeds than high-band 5G.



**Figure 2: 5G Local Cellular and Network Cellular**

<sup>2</sup> <https://developer.qualcomm.com/blog/spectrum-5g-innovation-boost-starts-here>

<sup>3</sup> <https://en.wikipedia.org/wiki/5G>



As transportation agencies evaluate their use of emerging cellular services, 5G technology is understood to be capable of performing low-latency, short distance communications for vehicle-to-vehicle or vehicle-to-infrastructure communications, as cellular-enabled vehicles and infrastructure become more widely deployed. Though the future of these technologies remains to be seen, 5G could supplement or replace Dedicated Short Range (DSRC) technology for connected vehicle applications. Use of 5G for long-distance data communications to field devices is also evolving.

Highlights from information gathered for this project, regarding current and expected use of 5G for transportation agencies' long-distance communications to field devices include:

- Buildout of 5G cellular is currently occurring primarily in urban areas.
- Most agencies are using or transitioning to 4G LTE for field device communications and do not anticipate using 5G for long-distance communications to field devices in the near future.

Cellular service carriers are deploying and testing 5G for multiple uses. “Smart Cities” deployments that include traffic and/or connected vehicle functions are relevant for transportation applications. Examples of 5G deployments, as noted by the cellular service carriers that participated in this project, include:

- **AT&T** – AT&T is developing, testing, and deploying 5G use cases with business customers, including The Washington Post<sup>4</sup>, AT&T Stadium<sup>5</sup>, and Purdue University. Purdue University is working with AT&T to create a test bed for 5G-based research and development at its Purdue Research Lab. The lab will use AT&T’s 5G+ millimeter wave (5G+) and commercially available Multi-access Edge Computing (MEC) technologies to help solve challenges like disaster recovery in rural, agricultural areas and explore new use cases for areas where business and community intersect – like smart cities.<sup>6</sup>
- **Verizon** – Verizon is working with the Mcity Test Facility in Michigan to advance transportation safety and shape the future of autonomous vehicles and smart cities using 5G. Verizon is testing 5G solutions designed to boost pedestrian safety and avoid car accidents. Adding Verizon 5G to the Mcity facility required installing 5G-connected cameras at every intersection to help identify traffic and pedestrian patterns to prevent collisions.<sup>7</sup>

#### 4.2.2 First Responder Network Authority (FirstNet)

[FirstNet](#) is an independent authority within U.S. Department of Commerce. Authorized by Congress in 2012, its mission is to develop, build, and operate the nationwide, broadband network that equips first responders to save lives and protect U.S. communities.<sup>8</sup>

---

<sup>4</sup> [https://about.att.com/innovationblog/2019/11/att\\_washington\\_post.html](https://about.att.com/innovationblog/2019/11/att_washington_post.html)

<sup>5</sup> [https://about.att.com/story/2019/5g\\_at\\_att\\_stadium.html](https://about.att.com/story/2019/5g_at_att_stadium.html)

<sup>6</sup> [https://about.att.com/story/2019/att\\_purdue\\_5g.html](https://about.att.com/story/2019/att_purdue_5g.html)

<sup>7</sup> <https://mcity.umich.edu/verizon-5g-ultra-wideband-network-now-live-at-mcity-test-facility/>

<sup>8</sup> <https://firstnet.gov/about>

The concept of a nationwide wireless broadband network was initiated following the September 11, 2001 attacks in New York City and other locations. This event revealed fundamental problems with communications systems used by first responders. During the tragedy and response, these entities could not easily communicate across agencies, and land and mobile phone lines were overwhelmed by a high volume of calls. FirstNet was created as part of the Middle Class Tax Relief and Job Creation Act ([PUBLIC LAW 112–96](#))<sup>9</sup> and signed into law in 2012. The law allocated 20 megahertz of spectrum and \$7 billion to establish a broadband network dedicated to first responders.<sup>10</sup> In 2017, AT&T was selected through a 25-year public-private partnership agreement to build and operate FirstNet.<sup>11</sup> The buildout of FirstNet is underway (operational in many locations) and expected to be complete by 2022.<sup>12</sup> An online [FirstNet coverage map](#)<sup>13</sup> provides a visual overview of locations where FirstNet service is available.

The FirstNet network offers voice and data communications services, and transportation agencies can procure FirstNet as an extended primary user. During an emergency, the FirstNet dedicated band (Band 14) can be cleared and locked for FirstNet users, with two levels of access:

- Primary Users – Includes first responders such as law enforcement, firefighters, and paramedics.
- Extended Primary Users – Includes entities that could be called on to help support first responders and can include essential government services, education, transportation, and utilities.<sup>14</sup>

#### **State DOT Use of FirstNet:**

Transportation agencies have begun to procure FirstNet services for data communications to field devices. A few of the advantages noted with the use of FirstNet are lower costs, stability of pricing, data security through a virtual private network (VPN) tunnel, and expanded cellular coverage.

Advantages cited with use of FirstNet for data communications to field devices: lower costs, stability of pricing, data security, and a new opportunity for expanded cellular coverage.

Highlights from information gathered for this project about State DOT use of FirstNet include:

- **NHDOT** – NHDOT is an “early adopter” in terms of connecting ITS devices to FirstNet, with approximately 30 field devices connected. NHDOT updated modems at these field device sites, and FirstNet service has been working well. A VPN tunnel between the FirstNet data center and the NHDOT network provides a very secure connection for data protection.
- **ODOT** – According to a 2019 ENTERPRISE report, ODOT has begun transitioning some ITS devices (e.g. cameras, traffic signals, DMS) to FirstNet.<sup>15</sup> ODOT noted that the cost of cellular equipment

---

<sup>9</sup> <https://www.congress.gov/112/plaws/publ96/PLAW-112publ96.pdf>

<sup>10</sup> <https://firstnet.gov/about/history>

<sup>11</sup> <https://2014-2018.firstnet.gov/news/firstnet-partners-att-build-wireless-broadband-network-americas-first-responders>

<sup>12</sup> AT&T interview, Appendix B

<sup>13</sup> <https://www.firstnet.com/coverage.html>

<sup>14</sup> <https://firstnet.gov/public-safety/firstnet-for/other-users>

<sup>15</sup> [http://enterprise.prog.org/Projects/2019/ENT\\_PhasingOutLegacy/ITS\\_Report\\_FINAL\\_Oct2019.pdf](http://enterprise.prog.org/Projects/2019/ENT_PhasingOutLegacy/ITS_Report_FINAL_Oct2019.pdf)

and monthly service fees is lower with FirstNet, compared to other providers. FirstNet also provides stability of pricing since it is government-based and required to keep prices stable or to offer lower prices. ODOT's conversion to FirstNet has been simple and efficient, especially at devices where in-place modems were already supplied by AT&T, FirstNet's service provider.

- **Caltrans** – Caltrans District 4 (San Francisco Bay Area) is using FirstNet cellular service for some field devices. Caltrans noted that the buildout of FirstNet offers a new opportunity to expand cellular coverage and co-locate on radio facilities to serve multiple needs.

### 4.2.3 Low-Power Wide-Area Networks (LPWAN)

Low-power wide-area networks (LPWAN) or Low Power Wide Area (LPWA) networks represent a novel communication paradigm that offers wide-area connectivity for low power and low data rate devices.<sup>16</sup>

LPWAN could be used to communicate to ITS devices with low bandwidth requirements at a lower cost compared to more common types of cellular service.

Compared with more common cellular networks (e.g. Wi-Fi, 3G, 4G LTE), LPWANs support smaller data transfers over wider areas, making LPWANs an ideal type of network for Internet of Things (IoT) applications, such as agricultural management, work site monitoring, asset tracking, fleet management, environmental sensing, and Smart City or infrastructure applications.<sup>17</sup>

LPWAN could be a viable option for communicating to ITS field devices with low bandwidth requirements, at a lower cost than more common cellular services such as LTE that offers higher bandwidth capabilities.

As noted during an agency interview for this project, **MTO** is investigating the use of LPWAN, known as LTE-M cellular service, for communications to dynamic message signs. The advantages of LTE-M service noted by MTO are lower rate plans and additional back-end services, for example the ability to monitor devices, check usage, and manage devices. While it is anticipated that the bandwidth capability of LTE-M will be suitable for communicating to DMS, MTO will also test latency, coverage, and overall performance.

---

<sup>16</sup> <http://ziyang.eecs.umich.edu/iesr/papers/raza17may.pdf>

<sup>17</sup> <https://www.soracom.io/iot-definitions/what-is-lpwan/>

## 5.0 Selecting Communications Infrastructure

---

Many factors are used by agencies to determine the most appropriate communication mechanisms for ITS field devices and system deployments. As ITS technologies evolve, the corresponding communications needs are also changing. Edge computing solutions and cloud computing capabilities provide an option for agencies to move complex data processing functions to the field or to the cloud, as appropriate, which impacts bandwidth needs. Lastly, the emergence of CAV technologies has led agencies to consider and evaluate long-distance communications options for backhaul data transfers.

### 5.1 Selection Considerations

Nearly all agencies that provided input for this project indicated that the selection of communications to ITS field devices is determined on a case-by-case basis. While many noted a preference to utilize agency-owned fiber when possible, several factors are considered.

The primary factors for determining communication mechanisms for long-distance data communications to field devices are availability/coverage, bandwidth needs and capacity, cost, security, and reliability:

Primary factors for selecting field device communications:

- Availability/Coverage
- Bandwidth
- Cost
- Security
- Reliability

#### **Availability/Coverage:**

- Many agencies noted that communications types are often chosen primarily based on proximity to infrastructure (e.g. in-place fiber) or service (e.g. cellular) available at the site of the field device.

#### **Bandwidth Needs and Capacity:**

- Bandwidth needs of field devices, coupled with the bandwidth capacity of the available communication mechanism, is another important consideration. For example, applications such as live video streaming from traffic cameras require high bandwidth capacity. Devices such as DMS, traffic signals, and road weather systems require lower bandwidth capacity.
- Fiber is widely acknowledged as the best choice in terms of capacity to meet high-bandwidth device needs. However, other communications types (e.g. point-to-point radio, cellular, microwave) may suffice depending on the situation. Devices with lower bandwidth needs can often be met by many types of long-distance communications mechanisms.

#### **Cost:**

- Though cost is a consideration, agencies are often bound by the infrastructure or services available at the site. For example, a rural area may have spotty or no cellular coverage, requiring agencies to build infrastructure to that area. Another example is in a mountainous region where only one cellular carrier offers service there is no option to compare costs among carriers.

- Cost considerations must include both initial investment and ongoing costs such as maintenance or service fees.
- Fiber can be expensive to build; however once in place, the benefit to owning fiber can exceed the initial investment, justifying the cost over time.
- Cellular can be the most economical and feasible choice for lower bandwidth applications, compared to building new infrastructure.

#### Cost Considerations

- Agencies consider cost but are often bound by what is available at the site
- Fiber can be expensive to build, but benefits over time can justify initial costs
- Cellular can be economical and feasible for lower bandwidth applications

#### Security:

- **NHDOT** noted data security as a primary consideration when selecting field device communications.
- Fiber is highly secure, with many agencies indicating it is the most secure choice.
- Cellular services that offer data security mechanisms such as VPN are often procured, when available, to address data security.

#### Reliability:

- Reliability during high-use, critical periods such as weather events, emergencies, and evacuations was noted as a key factor by two agencies.
- **GDOT** and **FDOT** indicated a preference to build agency-owned networks, to increase reliability during critical events, noting that cellular service has become overloaded due to heavy vehicle traffic with cell phone use during these emergency events.
- It unlikely that cellular networks would be expanded to fully meet needs during these rare events.

Improving reliability during critical events has prompted some agencies to build and maintain their own communications networks.

## 5.2 Tradeoffs with Ownership versus Leasing or Procuring Services

When weighing the pros and cons of agency-owned communications infrastructure assets versus leasing or procuring services, several preferences and tradeoffs were noted by agencies that provided input for this project. The following selection considerations, in addition to those identified in Section 5.1 above, were noted.

#### Capital Funds versus Operating Funds:

- Within transportation agencies, capital funding can be easier to obtain than operating funds, making it attractive to build and own communications infrastructure.
- Long-term operating costs for procured services (such as cellular or leased fiber) can be expensive, and operating funds to pay ongoing fees are more difficult to secure.
- An added benefit with building fiber is providing service to state-owned buildings such as truck stations in addition to field devices, leveraging the capital investment for multiple purposes.

### Ongoing Fees with Leased Services:

- When leasing tower space or procuring services, ongoing costs need to be considered. Agencies cannot control escalation rates, and future charges are difficult to predict.
- When high-bandwidth continuous communications are required, such as for traffic cameras during traffic incidents or weather events, agencies need to consider cost implications of service rate plans (e.g. cellular) that include monthly fees plus usage charges.

### Maintenance:

- Fiber requires less maintenance because it is underground and not exposed to the outdoor elements compared to cellular modems.
- However, maintenance can be a challenge with owned fiber. The agency needs to locate, protect, and repair fiber lines when damage occurs (e.g. due to digging activities). The agency's information technology (IT) department needs to be well-prepared to deal with a large network of fiber and devices. Furthermore, it can be challenging to find and retain qualified staff to perform maintenance on agency-owned communications infrastructure assets.

## **5.3 Edge Computing, Cloud Computing, and Exception Communications**

ITS field devices are often operated from a central location such as a TMC, which for some applications requires continuous or nearly continuous communications to send data from devices to the TMC, process data, and send operational commands. Some agencies are implementing or exploring edge computing solutions or cloud computing services to move complex data processing functions to the field (i.e. edge computing) or to the cloud (i.e. cloud computing). In these cases, communications to field devices may be only “by exception” or “as needed.” These strategies are utilized for multiple reasons, for example:

- Edge computing enables low-latency data processing for time-critical, on-site device operations.
- Cloud computing can allow traffic operators to access systems and initiate device commands from anywhere, functioning like a virtual TMC.
- Data processing at the field site or in the cloud can simplify operations and condense large datasets to alleviate centrally located data storage needs.
- When considering the benefits for agency infrastructure, edge or cloud computing strategies can reduce the need for continuous communications, which conserves bandwidth and makes a wider range of communications options available; for example, alternatives to fiber could be used to handle the resulting lower bandwidth data transfers.

Edge or cloud computing strategies can decrease the need for continuous communications, which conserves bandwidth and makes a wider range of communications options available.

As noted by the participating agencies, cellular is a viable option for devices that require only “exception” or “on-demand” communications. Following are examples where agencies are using or considering edge computing and cloud computing for various ITS devices and applications:

- **MTO** – MTO is de-centralizing complex data processing functions by performing data processing in the field (i.e. edge computing) or in the cloud (cloud computing) for some applications, as noted below. While some data processing will continue at a central location, edge and cloud computing can conserve bandwidth and decrease reliance on fiber.
  - Field Traffic Master (FTM) units complete data processing in the field for ramp metering, travel times on DMS, and DMS messages.
  - Third-party data providers provide travel times that can be downloaded directly to a field unit to trigger DMS displays without need to continuously communicate to a TMC.
  - An automated signing strategy determines DMS messages using an off-the-shelf application that operates in the cloud and is accessed from anywhere by traffic operators. Cellular is used to communicate by exception for over-rides to automated parameters.
  
- **GDOT** – Due a concern about storage capacity for large connected vehicle (CV) datasets at the DOT, GDOT is exploring edge computing solutions and/or increased processing capabilities at a central location.
  
- **MnDOT** – Edge computing is used at a pump station that communicates by exception to notify MnDOT dispatch when flooding is detected and for MnDOT to access system performance data. Other options are being investigated, including:
  - Tolling enforcement: Potential use of edge computing is driven by a need to quickly process a visual record of offenders on-site.
  - CAV data management: CAV applications will generate large volumes of data that can be processed in the field to produce smaller, manageable datasets for transfer to a central location. Processing at the edge also offers a security advantage as nominalizing CAV datasets will help with privacy by making the data less trackable.
  
- **WisDOT** – On-site (i.e. edge) computing is used for safety systems that require low latency data processing (e.g. wrong way, over height) and these systems are typically connected using cellular.
  
- **NHDOT** – Cellular is commonly used for devices that require “on-demand” communications (i.e. not continuously communicating) especially where it is not feasible to splice into fiber.

MTO is de-centralizing complex data processing functions by performing data processing in the field or in the cloud for some applications. Edge and cloud computing can conserve bandwidth and decrease reliance on fiber.

ITS Applications well-suited for Edge or Cloud Computing

- Travel times on DMS
- Tolling enforcement
- Real-time remote monitoring
- Time-critical safety systems
- CAV data management

## 5.4 Connected Vehicle Backhaul

Many transportation agencies have begun to deploy, test, and operate CV applications on their roadway networks. While much of the data processing and communications for these applications could occur in the field and/or in the vehicle itself, long-distance data communications using agency-operated backhaul infrastructure is likely needed to monitor devices in the field, send data to the site from a central location, and obtain valuable data from vehicles.

The following are key findings regarding long-distance communications for CV backhaul:

Fiber is preferred for CV backhaul and considered adequate for current and future needs. In the future, cellular could be used for both short-range and long-distance CV communications.

- **Selecting CV Backhaul:** Most agencies indicated that fiber is preferred for long-distance CV backhaul communications, and cellular is often used where fiber is not available. Selection considerations include security, reliability, capacity, and bandwidth needs driven by where data processing occurs and the volume of CV data transferred. Though fiber is largely the preferred choice for CV backhaul, in the future it is possible that cellular could be used for both short-range vehicle-to-infrastructure communications and backhaul communications. If cellular is used for CV data communications, there is a need to consider whether this additional bandwidth requirement will put too much load on cellular towers, especially in urban areas.
- **Performance:** Most agencies reported that long-distance CV data transfers primarily include low-volume data transfers that can easily be handled using fiber for backhaul. Initial testing of cellular for CV backhaul has been successful in areas where cellular service is strong and as low-volume data transfers (e.g. for device monitoring and intermittent viewing) are required.
- **Managing the Volume of CV Datasets:** Efforts to deploy solutions in which CV data processing occurs in the field (edge computing) can reduce the volume of data that is transferred to a central location via long-distance communications mechanisms, conserving bandwidth for data backhaul and reducing the need for extensive storage at a central site.
- **Future Planning:** Most agencies reported limited or no plans for expansion of communications infrastructure specifically to meet anticipated CAV backhaul needs.

Edge computing solutions that process and package CV data in the field can reduce the volume of data transferred to a central location, conserving bandwidth and reducing data storage needs at a central site.

Highlights from agency interviews regarding CV backhaul, including preferences, performance of current deployments, and future plans, include:

- **GDOT** – GDOT’s CV deployments are mostly connected to fiber for backhaul, with some connected to cellular where fiber is not available.



GDOT has deployed more than 600 roadside units (RSUs) in the Atlanta metro area. All RSUs communicate signal phase and timing (SPaT) and roadway geometry (MAP) data, with some transit signal priority and emergency vehicle preemption.

- Data processing occurs locally at the intersection.
- Routine data transfers are limited to low volumes of data for remote monitoring, management, and RSU updates.
- During testing to communicate large volumes of CV data from RSUs to the DOT, fiber backhaul was adequate. However, there is concern about storage space at the DOT for these large datasets.
- GDOT conducted a test in which SPaT and MAP data were streamed through the internet using cellular to test latency and bandwidth. Cellular performed well, with a strong LTE cellular network and relatively small volumes of data communicated.

GDOT streamed SPaT and MAP data through the internet using cellular to test latency and bandwidth. Cellular performed well, with a strong LTE network and relatively small volumes of data transferred.

A new GDOT CV deployment (6 RSUs on rural I-85) in partnership with Panasonic will soon be operational to test queue warning and weather incident warning.

- Data processing occurs at the roadside for time-critical applications.
  - CV data is communicated from the roadside to Panasonic's cloud datacenter for processing and analytics. Static and dynamic data messages are sent from the Panasonic centralized platform to the roadside.
  - 4G cellular is used for CV data backhaul, as fiber is not available in the area.
  - Initial testing of cellular for long-distance CV data communications was successful. Cellular coverage in the area is good, and low volumes of data are being transferred.
- **MDOT** – MDOT has deployed approximately 400 RSUs in the Detroit area. Most RSUs and related devices (e.g. cameras, detectors) are connected to fiber for backhaul; one corridor is on cellular. A typical CV site communicates 3-4 MB per second and is accessed by a central site for brief periods of time. Current backhaul infrastructure is sufficient for this volume of data, but the amount of data transferred for CV applications may increase over time. There are no current plans to change or expand communications infrastructure to accommodate CV backhaul.

- **MTO** – MTO will soon test 4G LTE cellular for CV backhaul with a deployment of up to 20 RSUs in Toronto. In terms of long-term planning, MTO will consider multiple options for CV backhaul including fiber and cellular. Considerations include security, reliability, capacity, and bandwidth needs:

MTO's considerations for selecting CV backhaul include security, reliability, capacity, and bandwidth requirements based on where CV data processing occurs – in the field, in the cloud, or at a central location.

- Fiber has been the most secure and reliable option historically.
- There is a need to consider if bandwidth use for CV backhaul will put too much load on cellular towers in urban areas.
- Backhaul choices will depend upon bandwidth required, based on where data processing occurs (e.g. in the field, in the cloud, or at a central location such as a TMC).
- CV backhaul could include a hybrid approach, using both fiber and cellular.

- **UDOT** – UDOT has CV deployments along two urban corridors with instrumented intersections to enable signal priority for buses and snowplows. A deployment in partnership with Panasonic is installing RSUs, equipping fleet vehicles with onboard units, building applications to utilize CV data, and building a cloud-based data analytics platform to process CV data.

- UDOT's CV deployments utilize fiber for backhaul.
- Fiber is preferred, as it is widely available in many areas and UDOT wishes to maintain the ability to transfer large volumes of data.
- UDOT expects its fiber network to have adequate capacity to transfer CV data and support other field device communications needs.

UDOT is using fiber for its urban and rural CV deployments. Fiber is preferred as it is widely available in many areas and UDOT wishes to maintain the ability to transfer large volumes of data.

- **MnDOT** - MnDOT is conducting a study to assess bandwidth capacity statewide and is developing a tool to track communications needs and capacity, including for CAV data backhaul. CAV data processing in the field (edge computing) will reduce the volume of data communicated via backhaul, conserving bandwidth and enhancing data privacy.
- **NDDOT** – NDDOT indicated that fiber is a viable option for CV backhaul. However, cellular could be used both for short-range vehicle-to-infrastructure communications as well as for backhaul, especially considering an FCC proposed rulemaking that would take away the DSRC spectrum dedicated for public safety. In rural ND, there is 95% coverage with Verizon which should be able to handle backhaul needs if cellular is used.

## 6.0 Long-term Management Practices

---

The long-term management practices used by agencies for obtaining, tracking, and managing communications infrastructure are many. In addition to managing agency-owned assets, some agencies have also had success in accessing communications assets and services through sharing or trading arrangements with the private sector. In addition, agencies often allow access to broadband providers to install facilities on DOT right-of-way or to co-locate equipment on agency-owned facilities, through agreements and/or permitting processes.

This section covers a wide range of agency practices, including:

- Permitting 5G small cell deployments on agency right-of-way
- Right-of-way access for broadband facilities and co-location on DOT towers
- Fiber sharing, resource trading, and public-private partnerships
- Fiber tracking
- Managing licenses and other assets

### 6.1 Permitting for 5G Small Cell Deployments in Right-of-Way

Current efforts by telecommunications providers to build out 5G cellular service has led to a need for state and local transportation agencies to implement policies and procedures for permitting of small cell wireless facilities in agency rights-of-way. Because high speed, low latency, 5G cellular service requires many antennas (i.e. small cells, or small wireless facilities) at close range, telecommunications providers are requesting access to install these facilities on the land adjacent to streets and highways owned by state and local agencies. Small cells can be installed on existing structures (e.g. utility poles, traffic signal structures, light poles) within public agency right-of-way or new structures may be built to mount this equipment.

A 2019 FCC rulemaking establishes shot clocks for agency review and approval of requests to install small wireless facilities on public rights-of-way, prompting agencies to develop related policies and procedures.

A 2019 U.S. Federal Communications Commission (FCC) rulemaking prompted transportation agencies to develop policies and procedures for allowing small wireless facility installations on the right-of-way, as in many cases policies did not include permitting for this type of facility. The [Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment](https://www.fcc.gov/document/fcc-facilitates-wireless-infrastructure-deployment-5g)<sup>18</sup> rulemaking established shot clocks for agency review and approval of small wireless facility requests and allows for agency cost recovery.

Policies and procedures vary by agency. Most agencies indicate a preference or even a requirement for small cell installations to be on newly constructed structures/poles, due to concerns (e.g., safety,

---

<sup>18</sup> <https://www.fcc.gov/document/fcc-facilitates-wireless-infrastructure-deployment-5g>

structural capacity) about mounting equipment on in-place DOT structures. Highlights from information gathered for this project about policies and procedures for small cell wireless installations on the right-of-way include:

Some agencies require or encourage small wireless facility (i.e. small cell) installations on newly constructed poles rather than on existing DOT structures.

- **TxDOT** – TxDOT created its Wireless Siting program in 2018, with input from the telecommunications industry. As of January 2020, nearly 500 small cell sites were approved by TxDOT, with the majority of approved installations on new poles.<sup>19</sup> TxDOT maintains a public website, [TxDOT Real Property Map](https://maps.dot.state.tx.us/AGO_Template/TxDOT_Viewer/),<sup>20</sup> that displays locations of small cell leases as a layer on the property assets map. Figure 3 shows a screenshot from the TxDOT Real Property Map.

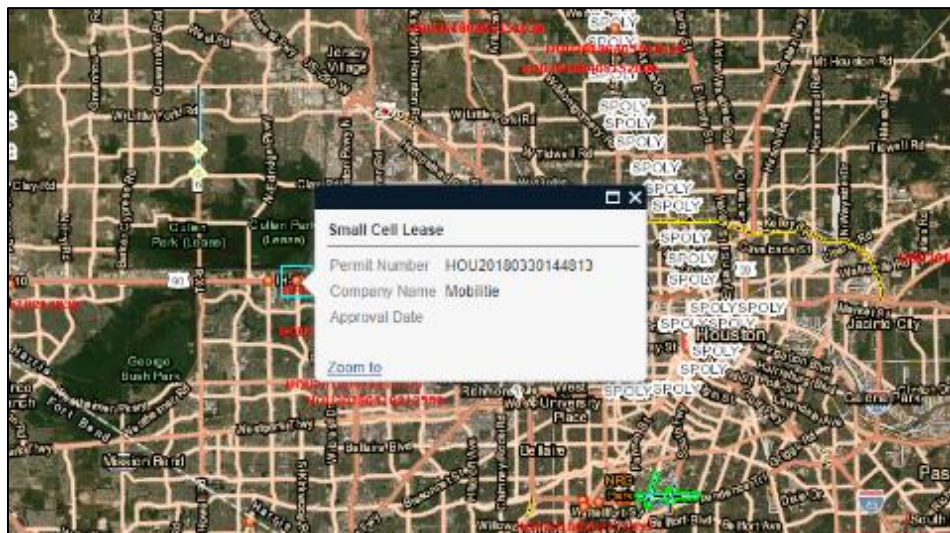


Figure 3: Screenshot from TxDOT Real Property Map website

- **DeIDOT** – DeIDOT has established detailed processes, checklists, forms, and workflows for wireless small cell permit requests. A Gatekeeping Checklist provides application submission requirements and a Technical Review Checklist outlines technical submittal requirements for each new or impacted structure. Requirements, checklists, and related resources are posted at the [DeIDOT Wireless Small Cell Permits](https://deldot.gov/Business/WirelessPermits/index.shtml)<sup>21</sup> web page, with the following application review timelines:
  - Gatekeeping/Completeness determination – 14 days for acceptance/rejection
  - Initial application technical review – 60 days, inclusive of the 14 days, if submission is deemed complete unless an extension is mutually agreed upon
  - Revised application review – 15 days if resubmitted within 30 days of denial

<sup>19</sup> TxDOT presentation, 2020 TRB Annual Meeting

<sup>20</sup> [https://maps.dot.state.tx.us/AGO\\_Template/TxDOT\\_Viewer/](https://maps.dot.state.tx.us/AGO_Template/TxDOT_Viewer/)

<sup>21</sup> <https://deldot.gov/Business/WirelessPermits/index.shtml>

DeIDOT utilizes a consultant to conduct reviews and works closely with the providers to negotiate each deployment. The most favorable outcomes for DeIDOT are when a small wireless provider co-locates on a utility-owned pole or takes ownership of a DeIDOT pole. The least preferred outcome is co-location at a DOT structure where DeIDOT retains ownership. Pre-submittal meetings with the requesting entities are an important tool to establish working relationships and understand the provider’s requirements.<sup>22</sup>

- **UDOT** – UDOT has posted processes for permitting and installing small wireless facilities (SWF) in the right-of-way on the [UDOT Small Wireless Facilities Permitting](#)<sup>23</sup> web page. The [SWF Installation Guidelines](#)<sup>24</sup> include drawings showing allowable SWF mounting locations on multiple types of DOT poles and indicates conditions in which co-location on DOT structures is not allowed. Figure 4 shows a page from the installation guidelines, with details for SWF mounting location on CCTV and non-intrusive detector poles.

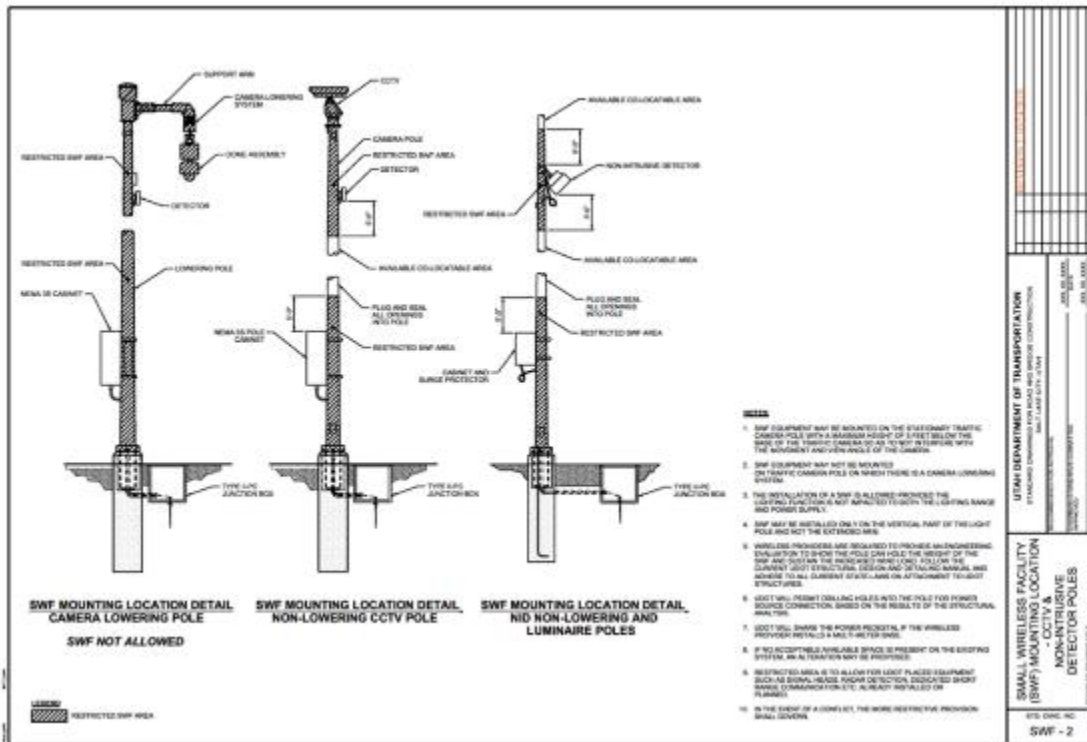


Figure 4: Details from UDOT Small Wireless Facilities (SWF) Installation Guidelines

UDOT maintains an online [Small Wireless Facilities Interactive Map](#)<sup>25</sup> showing locations of small cell facility permits, along with photos and details of small cell equipment that has been installed. Figure 5 shows a screenshot from the online map, along with photos of a small cell equipment

<sup>22</sup> DeIDOT presentation, 2020 TRB Annual Meeting

<sup>23</sup> <https://site.utah.gov/connect/business/permits/small-wireless-facilities-5g/>

<sup>24</sup> [https://www.udot.utah.gov/main\\_old/uconowner.gf?n=3475431509205008](https://www.udot.utah.gov/main_old/uconowner.gf?n=3475431509205008)

<sup>25</sup> [www.udot.utah.gov/go/smallwireless5Gmap](http://www.udot.utah.gov/go/smallwireless5Gmap)

installation. In terms of responsibility for future relocations of small wireless facilities, [Utah Code Chapter 21: Small Wireless Facilities Deployment Act](#)<sup>26</sup> states that an authority may require a wireless provider to relocate or adjust a small wireless facility in a public right-of-way in a timely manner and without cost to the authority owning the public right-of-way.



**Figure 5: Screenshots and Photos from UDOT Small Wireless Facilities Interactive Map**

- IDOT** – Small cell facility installation requests are treated as a standard utility installation (i.e. utility permit) and no fees are assessed. Small cell installations are not allowed on DOT-owned structures. An Illinois DOT memorandum containing internal agency guidance indicates minimum requirements for permit applications, such as site location, installation plans and specifications signed by a licensed structural engineer, power, and connectivity details. Other considerations include aesthetics, installation method, communications and electrical requirements, roadway clearances, and clearance to other existing DOT structures.<sup>27</sup>
- WisDOT** - Wisconsin statute [2019 Wisconsin Act 14](#)<sup>28</sup> allows cellular providers to install small wireless facilities in the right-of-way. WisDOT works with providers to request that they install their own poles rather than installing equipment on DOT-owned structures, and to keep electrical systems separate. Details for permit applications, rate/fee schedules, and related requirements can be found in the [WisDOT Highway Maintenance Manual](#).<sup>29</sup>

<sup>26</sup> [https://le.utah.gov/xcode/Title54/Chapter21/C54-21\\_2018050820180901.pdf](https://le.utah.gov/xcode/Title54/Chapter21/C54-21_2018050820180901.pdf)

<sup>27</sup> Illinois DOT memorandum

<sup>28</sup> <https://docs.legis.wisconsin.gov/2019/related/acts/14>

<sup>29</sup> <https://wisconsin.gov/Documents/doing-bus/real-estate/permits/09-15-41.pdf>

## 6.2 Right-of-Way Access, Co-Location, and Resource Sharing

Transportation agencies often grant access to other government entities and private broadband providers to install facilities in the highway right-of-way or co-locate equipment on DOT-owned facilities such as radio towers. Some agencies share infrastructure assets (e.g. fiber), enter into resource trading agreements, or utilize public-private partnerships to collaborate for network expansion and mutual benefit. These practices vary by agency and are often governed by state statutes.

### 6.2.1 Access to Broadband Facilities

Three agencies interviewed for this project noted long-standing and emerging practices related to allowing access to right-of-way for broadband development or accessing statewide broadband facilities. These practices vary in how they are mandated and carried out but tend to be driven by initiatives to encourage broadband development and leverage resources statewide. These practices include:

DOT practices for allowing right-of-way access tend to be driven by initiatives that encourage broadband development and leverage resources statewide.

- **Caltrans** – Caltrans has a master license agreement to allow cellular providers to lease space in the Caltrans right-of-way, with an associated cost. Recent California legislation allows broadband providers to install fiber or empty conduit in the right-of-way when Caltrans is doing highway work. Caltrans maintains an online [Map of Proposed Transportation Projects on the State Highway System](#)<sup>30</sup> for broadband providers to view upcoming projects.
- **NHDOT** – The [Network New Hampshire Now](#),<sup>31</sup> spearheaded by the University System of New Hampshire, is a collaboration between state and local governments, non-profits, and private entities to bring a mix of wireline and wireless next-generation broadband services to community anchor institutions in New Hampshire and to make broadband service more readily available to the state’s households and businesses. The State of New Hampshire (i.e. state agencies) has guaranteed access to this network with an associated cost.
- **WisDOT** – Wireless facilities such as cellular towers, monopoles, macro cells, small wireless facilities, and their associated equipment may be installed in the highway right-of-way, as outlined in the [WisDOT Highway Maintenance Manual](#).<sup>32</sup>

### 6.2.2 Co-location on DOT-owned Towers

Several agencies noted that they allow private wireless providers and/or other public entities to co-locate equipment (i.e. transceivers) on DOT-owned towers. **FDOT** has a unique agreement with a private sector

---

<sup>30</sup> <https://dot.ca.gov/programs/design/wired-broadband>

<sup>31</sup> <https://www2.ntia.doc.gov/grantee/university-system-of-new-hampshire>

<sup>32</sup> <https://wisconsin.dot.gov/Documents/doing-bus/real-estate/permits/09-15-41.pdf>

entity to manage subleases on DOT towers, on behalf of the agency. Relevant practices gathered during this project include:

- **MnDOT** – Cities, counties, and other public safety or governmental agencies can request to use space on MnDOT towers and shelters where there is excess capacity. Public safety entities are not assessed a fee for occupying space, but a nominal charge for power consumption is collected. Non-public safety and private entities may request to use capacity on towers where capacity is not required for public safety users, and a fee is assessed. Related policy and procedures are documented at the [MnDOT Statewide Radio Communications](#)<sup>33</sup> web page.
- **Caltrans** – Caltrans allows private broadband providers to co-locate on DOT-owned radio facilities, such as vaults and towers.
- **NDDOT** – NDDOT does not allow privately owned transceivers on DOT-owned towers. However, other government entities (e.g. federal agencies, state radio) are allowed to locate transceivers on DOT-owned towers.

FDOT's Lodestar agreement provides exclusive rights to market and sublease space on certain DOT towers. FDOT receives a percentage of the gross receipts from the subleases.

- **FDOT** – FDOT entered into a contract with American Tower known as [Lodestar](#)<sup>34</sup> which provides exclusive rights to market and sublease space on certain FDOT towers. Lodestar may enter into sublease agreements with wireless providers and provides FDOT with a percentage of the gross receipts derived from the subleases. This strategy encourages wireless service providers to co-locate on towers located primarily on FDOT's limited-access rights-of-way rather than developing numerous new tower sites in local communities.

### 6.2.3 Fiber Sharing, Resource Trading, and Public-Private Partnerships

Some transportation agencies are successful in accessing data communications assets and services through sharing arrangements with the private sector, including fiber sharing, resource trading, and public-private partnerships. The allowance of such arrangements is often governed by state law, and when allowed can leverage public and private resources for mutual benefit of all parties involved.

A previous ENTERPRISE study [Policies, Laws, and Agreements for the Use of Fiber Communications](#)<sup>35</sup> summarized resources (policies, laws, agreements) and state DOT practices for sharing fiber infrastructure. The study documented a long history of state laws and practices for sharing fiber assets with public entities (commonly cities, counties, and universities) and private telecommunications providers. A survey of U.S. state and Canadian provincial transportation agencies revealed that 11 of 14

---

<sup>33</sup> <http://www.dot.state.mn.us/oec/>

<sup>34</sup> <https://www.fdot.gov/traffic/its/projects-telecom/lodestar.shtm>

<sup>35</sup> [http://enterprise.prog.org/Projects/2015/fiber/ENT\\_Fiber\\_Communications\\_FINAL\\_Report\\_Dec2016.pdf](http://enterprise.prog.org/Projects/2015/fiber/ENT_Fiber_Communications_FINAL_Report_Dec2016.pdf)



responding agencies participate in a variety of fiber sharing arrangements. Arrangements that provide transportation agencies with access to fiber that they do not build or own can take several forms, including gaining access to a telecom provider’s fiber network in exchange for occupation of highway right-of-way or trading access to fiber on the other’s network. Public-public sharing arrangements rarely include exchange of funds and are often seen as mutually beneficial to improving traffic operations by connecting traffic control devices and ITS assets. Sample fiber sharing agreements made available to the project from Iowa DOT, Virginia DOT, and WisDOT are posted on the [ENTERPRISE website](#).<sup>36</sup>

Relevant highlights from information gathered for this project include:

- **WisDOT** – Wisconsin law allows WisDOT to obtain fiber assets from broadband providers in exchange for access to install fiber in the right-of-way. This arrangement has contributed to WisDOT’s robust fiber network for ITS field device communications around the state.
- **UDOT** – UDOT enters into resource trading arrangements with multiple private telecommunications companies. Exchanges take various forms, for example, trading use of DOT strands for use of telecom-owned strands or allowing providers to install fiber on UDOT right-of-way (ROW) in exchange for UDOT use of provider-owned fiber. Resource exchanges may or may not be in the location of the negotiated installation. In a recent agreement with UDOT, Crown Castle International proposed a distributed antenna system (DAS) in the Cottonwood Canyons, and the resource exchange included:<sup>37</sup>

Wisconsin DOT’s practice of obtaining fiber from broadband providers in exchange for right-of-way access has contributed to WisDOT’s robust fiber network.

Crown Castle International received:

- Build fiber-optic backbone in ROW
- Wireless poles in ROW
- Use of UDOT fiber conduit
- Hub building on UDOT ROW

UDOT received:

- 24 strands on fiber cable
- Spare conduit
- Access to all poles for equipment
- RWIS installation
- Power for devices
- Hub space for equipment



**Figure 6: Distributed antenna system in Cottonwood Canyon, Utah (Source: Utah DOT)**

<sup>36</sup> [http://enterprise.prog.org/Projects/2015/fiber\\_communications.html](http://enterprise.prog.org/Projects/2015/fiber_communications.html)

<sup>37</sup> UDOT Fiber Optic Update 2019. Presentation.

- **MnDOT** – MnDOT shares fiber with another state agency, Minnesota IT Services, which provides connectivity to state, county, and city entities. MnDOT generally shares dark fiber stating clear lines of responsibility, which limits security concerns.
- **GDOT** – GDOT is planning for a statewide fiber network, aiming to establish a public-private partnership model for broadband development that implements a combination of agency-owned and privately owned fiber along the interstates.
- **Arizona DOT** – Arizona DOT (ADOT) is exploring partnerships that would lead to development of fiber-optic infrastructure, creating more affordable opportunities for wired and wireless broadband connectivity in rural communities. ADOT plans to use the fiber to provide “smart highway” technology (e.g. overhead message boards, traffic cameras, weather stations, wrong-way driving detection) and will help lay the groundwork for emerging technology such as connected and automated vehicles.<sup>38</sup>
- **AT&T Public-Private Partnerships** – AT&T is flexible in developing public-private partnerships to exchange goods or services. For example, AT&T has provided “smart cities solutions” (e.g. smart lighting elements on poles, digital kiosks, public Wi-Fi access in parks) in exchange for access to agency right-of-way, reduced permitting times, or waived permit fees. In another example, AT&T is providing a roadside unit as part of a small cell deployment in exchange for right-of-way access. A public-private partnership initiative with the City of San Jose, California includes a strategic collaboration for deployment of small cells, with a pilot to trial AT&T Smart Cities solutions.<sup>39</sup>

Georgia DOT and Arizona DOT are seeking public-private partnerships to expand broadband development across their states.

### 6.3 Fiber Tracking

Transportation agencies that own, lease, or share fiber with other entities need to understand the locations and characteristics of these assets on an ongoing basis as networks expand and change. Agencies that track fiber locations and attributes may use in-house tools (e.g. spreadsheets, databases, mapping tools) or off-the-shelf products. Agencies that systematically track fiber networks often utilize geographic information system (GIS) tools to display related information.

Highlights regarding fiber tracking tools documented for this project include:

- **FDOT** – The [ITS Facilities Management \(ITSFM\)](https://www.fdot.gov/traffic/itsfm/newusersagencies/about-itsfm)<sup>40</sup> system is an asset, configuration, and document management system. ITSFM compiles asset information into a single, accessible GIS-based graphical and tabular database. FDOT has an enterprise license for the ITSFM configuration of Byers Engineering Company’s [NexusWorx](http://nexusworx.byers.com/)<sup>TM 41</sup> product. Fiber assets tracked in ITSFM include:

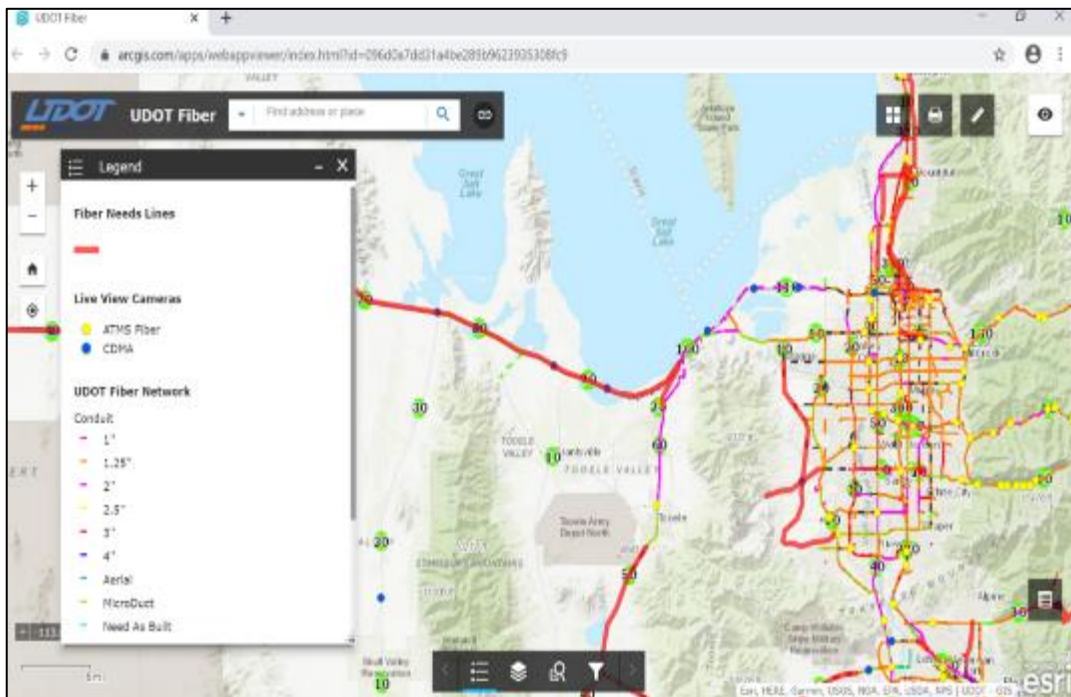
<sup>38</sup> <https://azdot.gov/adot-news/state-seeks-input-leveraging-broadband-expansion-along-highways>

<sup>39</sup> [https://about.att.com/story/san\\_jose\\_public\\_private\\_partnership.html](https://about.att.com/story/san_jose_public_private_partnership.html)

<sup>40</sup> <https://www.fdot.gov/traffic/itsfm/newusersagencies/about-itsfm>

<sup>41</sup> <http://nexusworx.byers.com/>

- Geographic location and feature attributes: conduit duct banks and access points
  - Fiber cable:
    - Fiber cable type, size, year installed
    - Fiber utilization (i.e. working, defective, reserved)
    - Fiber splice and termination
  - Fiber patch panel assignments
  - Fiber path trace for dark fibers and active circuits
  - Outage locate tool to quickly determine fiber outage locations
- **GDOT** – GDOT uses the NexusWorx™ product for fiber tracking.
  - **UDOT** – UDOT tracks its fiber network using Bentley for the backend database. The data is converted to Esri [Arc-GIS](https://www.esri.com/en-us/arcgis/about-arcgis/overview)<sup>42</sup> for web viewing. An Esri server located at UDOT improves the quality of map viewing. The online [UDOT Fiber Map](https://www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9)<sup>43</sup> displays conduit size, location, length, owner, planned fiber lines, and splice details, and is used by UDOT and its partners for planning, locates, and trouble-shooting. While most data is available via the online map, credentials are required to access IP plans and as-builts. Figures 7 and 8 show screenshots from the UDOT Fiber Map.



**Figure 7: Screenshot from the UDOT Fiber Map Showing Current Fiber Lines and Fiber Needs Lines**

<sup>42</sup> <https://www.esri.com/en-us/arcgis/about-arcgis/overview>

<sup>43</sup> [www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9](https://www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9)



## 6.4 Managing Licenses and Agreements

Many transportation agencies obtain licenses from the Federal Communications Commission (FCC) for use of the electromagnetic spectrum for technologies such as two-way radios and ITS field devices that communicate using radio or microwave. As such, agencies need to maintain these FCC licenses on an ongoing basis. In addition, agencies that allow non-DOT entities to co-locate equipment on their facilities have a need to track and manage agreements for these co-locations.

### 6.4.1 FCC Licenses

Transportation agencies typically assign dedicated staff to obtain and manage FCC licenses, such as renewal timelines and other license details. Following are examples of how agencies manage FCC licenses.

- **NDDOT** – NDDOT utilizes RadioSoft (contractor for [AASHTO's Frequency Coordination Program](#)) for FCC spectrum coordination, which is helpful for tracking licenses.
- **Caltrans** – The California Office of Emergency Services tracks all FCC licenses statewide. At Caltrans, FCC licenses are tracked in a database and in a physical file for each license.
- **MnDOT** – The MnDOT Office of Statewide Radio Communications' engineering group obtains and manages FCC licenses. Staff actively monitor licenses for renewals and utilize the FCC's database and related notifications to manage licenses.
- **FDOT** – FCC licensing is verified and/or maintained via the Central Office TSM&O under a scope of work issued to FDOT's Telecommunications General Consultant contractor.
- **NHDOT** – NHDOT has dedicated staff who obtain, manage, and maintain FCC licenses, utilizing processes such as regular reviews and calendar reminders for required notifications to the commission and renewal opportunity windows.

### 6.4.2 Co-location Agreements

Some agencies enter into agreements to allow private companies or other government entities to co-locate equipment on DOT facilities such as radio towers. In these situations, agencies need to track and document the details of equipment installed and the terms of associated agreements. Following are examples of tracking co-location agreements.

- **Caltrans** – Each co-location on DOT-owned radio facilities is tracked and contains details such as the provider information and type of equipment. All cellular co-locations on DOT facilities are also tracked via site license agreements.
- **MnDOT** – MnDOT tracks tower space leases through formal agreements in MnDOT's document management system. Locations are tracked in a database and in as-builts.

## 7.0 Security

---

As transportation agencies' ITS networks and communications systems are expanded and become more complex in nature, it is necessary for proper security measures to be implemented. This section describes physical security tactics and cybersecurity strategies for ITS communications networks, including a summary of recently published resources that provide technical guidance and recommended practices for cybersecurity as tailored for transportation agencies, TMC facilities, and ITS networks.

### 7.1 Physical Security – Agency Practices

Many agency practices for physically securing ITS devices and systems were shared during information-gathering for this project. The practices include tools for monitoring field devices and communications networks, and tactics for security of field boxes, shelters, cabinets, towers, and tower buildings.

#### 7.1.1 Monitoring Field Devices and Communications Networks

Monitoring field devices and communications networks remotely is critical for agencies to know when components may not be properly functioning. Below are examples of monitoring tools.

- **MnDOT** – MnDOT uses a Network Management System (NMS) for monitoring long haul communications. Since field devices are online, MnDOT staff can clearly see when devices have gone offline, indicating a problem.
- **NHDOT** – NHDOT uses [SolarWinds](#)<sup>® 44</sup>, a software platform for networks, to monitor network usage and identify issues.

#### 7.1.2 Field Boxes, Shelters and Cabinets

Physical security of field boxes, shelters, and cabinets is critical for agencies to protect equipment from vandalism or security breaches. Common tactics include changing out standard/universal keys, using electronic lock systems or multiple locks, and modifying equipment placement (e.g. burying underground or high mounting). The following includes examples of tactics used by agencies to secure field device components housed in boxes, shelters, and cabinets.

##### Security Tactics for Boxes, Shelters and Cabinets

- Change out universal keys
- Electronic lock systems
- Multi-lock access
- Burying or high mounting of equipment

- **NDDOT** – The [NDDOT standard specifications](#)<sup>45</sup> for boxes that house components to support field devices include provisions to deter vandalism. For example, increased depth to house more

---

<sup>44</sup> <https://www.solarwinds.com/>

<sup>45</sup> <https://www.dot.nd.gov/divisions/environmental/docs/supspecs/2014StandardSpecifications.pdf>

equipment in a single box, no longer using a universal key for access, and mounting boxes higher so lift equipment is needed to access equipment for maintenance.

- **Caltrans** – Pull boxes are buried deeper to decrease instances of vandalism. See [Caltrans standard specifications](#)<sup>46</sup> for Pull Boxes (86-1.02C) and Installation of Pull boxes (Sect 87-103C).
- **MnDOT** – Shelters and DMS have changeable key cores that are changed out after construction. There is also an option to add padlocks to equipment cabinets and pole cabinets. MnDOT communications shelters have key card access and a monitoring system.
- **NHDOT** – NHDOT staff make frequent visits to remote sites to check on field equipment. NHDOT uses alternate locks to traffic cabinets rather than standard locks that come with the cabinet.
- **UDOT** – UDOT is replacing all field cabinet locks with an electronic lock system. Each staff has a key with an RFID chip registered to that person, giving them access to the cabinet for a selected period of time (e.g. 7 days). When this time elapses, staff are required to log in to re-register the key. This system also generates a log of all activity for each key.

### 7.1.3 Towers and Buildings

Security at a DOT communications facilities, such as towers and tower buildings, can be accomplished through alarms and monitoring access, as described in the examples below.

#### Security Measures for Towers and Tower Buildings

- DOT staff accompany co-locating entities into facility
- Dual locks
- Alarms on doors
- Real-time access verification
- Entry/exit logs
- Pre-established clearances

- **NDDOT** – When other government entities co-locate transceivers on DOT-owned radio towers, NDDOT accompanies their staff to the equipment as needed. An alarm system is present on tower building doors.
  - **Caltrans** – An alarm alerts the statewide operations center when a door is opened at a radio tower, allowing those entering and exiting to identify themselves and to log entries and exits to the tower. Caltrans radio coordinators typically accompany individuals from co-locating entities that request access to DOT-owned radio towers.
- **MnDOT** – MnDOT practices for radio tower security include:
    - Staff in MnDOT’s Radio Operations Center monitor tower sites 24hours/day, 7 days/week, 365 days/year. Tower sites are gated. All entities that have co-located equipment on towers are required to contact the Radio Operations Center when they check in and out.

---

<sup>46</sup> <https://dot.ca.gov/programs/design/ccs-standard-plans-and-standard-specifications>

- Radio sites have a card key system and a key/deadbolt, for dual access.
- Equipment shelters have an alarm system on the doors.
- **FDOT** – Access into facilities requires Department of Homeland Security (DHS) Level 2 / Criminal Justice Information Services clearances for all personnel. All third-party leases at FDOT are required to have their own shelter and electrical power on co-located tower sites. State, City and/or County Public Safety co-locates are provided with access under FDOT’s Tower/Shelter Use Agreements under the same security requirements.

## 7.2 Cybersecurity – Agency Practices and Cellular Service Protections

Cybersecurity is a high priority for transportation agencies as technologies continue to evolve and change. This section provides overall general cyber security practices of transportation agencies as well as connected vehicle infrastructure and data security cybersecurity practices.

### 7.3.1 General Cybersecurity Practices

Following are cybersecurity practices (e.g. firewalls, virtual private networks) noted by transportation agencies interviewed for this project.

- **NHDOT** – NHDOT ensures that software patches to equipment/devices and communications infrastructure are current.
- **UDOT** – The UDOT ATMS network (e.g. fiber, field devices) is not directly connected to the internet, securing it from external hacking.
- **WisDOT** – WisDOT has worked with Verizon to obtain a VPN which isolates the agency’s cellular network from the public network, typically for signals and portable devices. For devices connected to the public network, the connection is password protected if a connection to an IP address is needed. Factory default passwords are removed from field devices to mitigate hacking into devices.
- **MnDOT** – Most field devices are on a VPN with Verizon.
- **NHDOT** – A VPN tunnel between the FirstNet data center (AT&T) and NHDOT network provides a very secure connection for data protection.
- **MDOT** – Cellular modems are currently on public IPs, but these will soon be moved to private IPs with Verizon, to increase security.

#### General Cybersecurity Practices

- Virtual Private Networks (VPNs) for cellular service
- Ensure current software patches
- ITS network not connected to the internet
- Remove factory default passwords from field devices



### 7.3.2 Connected Vehicle Infrastructure and Data Security

As connected vehicle technologies and communications evolve, agencies are increasing the security of connected vehicle data and implementing measures to secure roadside units that, when widely deployed, could increase access points into DOT-operated networks. Examples of security for connected vehicle applications are provided below.

- **GDOT** – For RSUs connected to cellular for backhaul, a secure tunnel within the cellular provider’s network offers a private connection for long-distance data transfers. Security credentialing (SCMS) is used to verify CV messaging.
- **MDOT** – There is a concern that RSU sites which broadcast wirelessly could be hacked, potentially exposing the statewide network to security vulnerabilities. MDOT is exploring security mitigation measures at the server end of CV communications.

Physical security is a high priority for CV deployments. Many RSUs in the field could create numerous access points into DOT networks.

#### CV Security Strategies

- RSUs on cellular - VPNs and built-in firewalls
- Lock down access to RSUs in the field
- Security credentialing for CV messages

- **MTO** – Security is a high priority because there will be many more access points with multiple RSUs deployed for CAV operations. Security strategies include acquiring LTE modems with built-in firewalls, locking down access to ports in switches within field cabinets (e.g. MTO staff or contractors will only be able to plug into a port with an authenticated laptop), and implementing additional security measures in rural areas.
- **UDOT** – The [Security Credentialing Management System \(SCMS\)](#)<sup>47</sup> will be used to secure the transmission of CV messages for the Panasonic deployment.

### 7.3.3 Cellular Service Cybersecurity Protections

As noted in the previous sections, VPNs are often offered by cellular service carriers and utilized by agencies to isolate field devices from public cellular networks. Additional cybersecurity protections, as shared by AT&T through an interview for this project, include:

- **Network Security:** Network security follows globally defined standards and allows for customizable options to add additional layers for AT&T’s Enterprise customers such as private IP address pooling, and Multiprotocol Label Switching (MPLS) connectivity between networks.
- **User Managed Security:** Options exist to create closed user groups (e.g. no one can send an SMS unless they are in the user group, lock down peer to peer).
- **Threat detection/intelligence:** AT&T Alien Labs Open Threat Exchange, the threat intelligence unit of the company’s cybersecurity organization, delivers analytics-based intelligence for resilient

<sup>47</sup> <https://www.its.dot.gov/resources/scms.htm>

threat identification and response situations, for example, if a connection or a device is hacked, an immediate action to the break wireless connection can be initiated.

## 7.2 Cybersecurity Resources

This section identifies recent research focused on cybersecurity at TMCs and field devices. At the project onset, two primary U.S. national studies sponsored by the U.S. Department of Transportation (USDOT) and the National Cooperative Highway Research Program (NCHRP), respectively, were identified for review, to provide a well-rounded overview of cybersecurity best practices for traffic/ITS operations:

- [\*Transportation Management Center Information Technology Security\*](#) (Toppen et al., 2019):<sup>48</sup> This report, published by USDOT, provides recommended practices and guidelines for cybersecurity at TMCs.
- [\*NCHRP 03-127 Cybersecurity of Traffic Management Systems\*](#) (2019):<sup>49</sup> This research developed guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (e.g. traffic signal systems, ITS devices, vehicle-to-infrastructure systems).

Two additional notable resources were identified, as shown below with a brief overview of each:

- [\*NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems\*](#) (July 2020).<sup>50</sup> The U.S. National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency recently released a joint advisory for critical infrastructure Operations Technology and control systems, to raise awareness of current cyber threats and provide related recommendations.
- [\*Cybersecurity and Intelligent Transportation Systems: Best Practice Guide\*](#) (Krause et al., 2019):<sup>51</sup> This report, published by USDOT, presents best practices in ITS cybersecurity – specifically in planning and conducting a penetration test. The objective of an ITS penetration test is to identify exploitable vulnerabilities in the DOT ITS environment, categorize the severity of the vulnerabilities, and receive experienced recommendations for mitigating risks. This report details the methodology of scoping a penetration test and provides a template test plan to start local and state DOTs in their own cybersecurity plan and test.

The first two primary resources, *Transportation Management Center Information Technology Security* (focus on TMCs) and *NCHRP 03-127 Cybersecurity of Traffic Management Systems* (focus on field devices), are summarized below.

---

<sup>48</sup> <https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf>

<sup>49</sup> <https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179>

<sup>50</sup> <https://us-cert.cisa.gov/ncas/alerts/aa20-205a>

<sup>51</sup> <https://rosap.ntl.bts.gov/view/dot/42461>

### 7.2.1 Transportation Management Center Information Technology Security

The [Transportation Management Center Information Technology Security](#) report provides practices, experiences, and lessons learned from IT and other industries and applies them to a TMC context. It presents insight into basic practices that can serve as a starting point for organizations with limited resources and cybersecurity expertise, as well as guidelines for TMCs looking to increase their system maturity. Highlights retrieved from this report include:

- **Basis for TMC Cybersecurity Practices:** The TMC cybersecurity practices presented are based on best practices, with a focus on the [Center for Internet Security \(CIS\) Top 20 Controls](#).<sup>52</sup> The CIS Controls™ are a prioritized set of actions that collectively form a defense in depth set of best practices that mitigate the most common attacks against systems and networks. Figure 10 lists the CIS Controls™, organized by basic, foundational, and organizational controls.

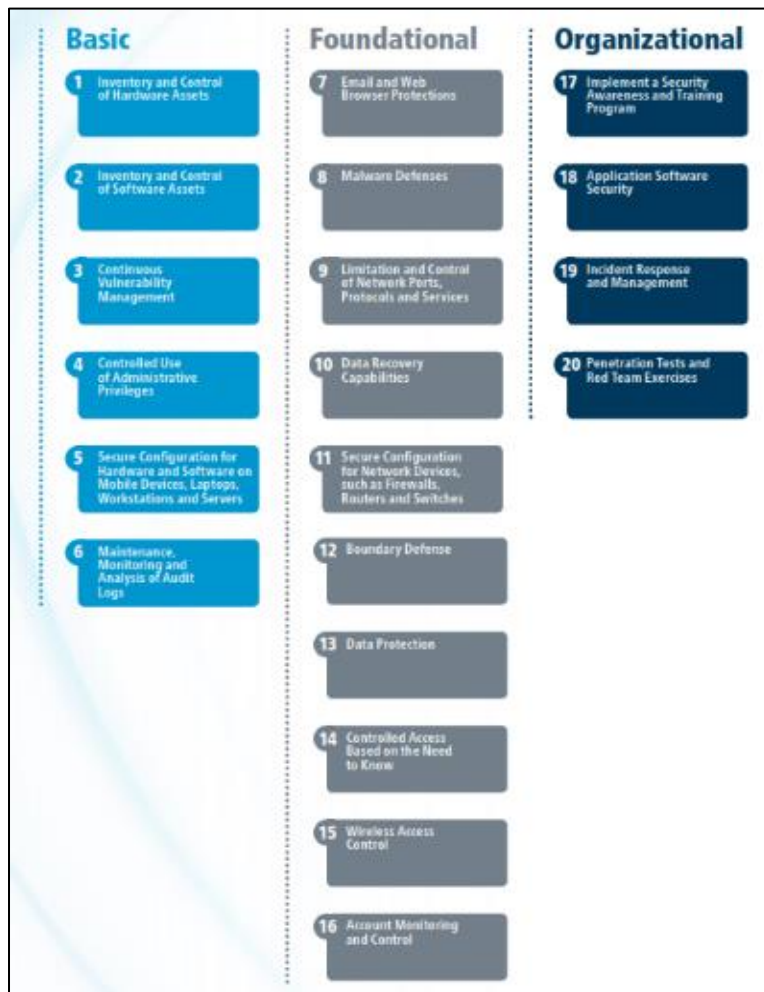
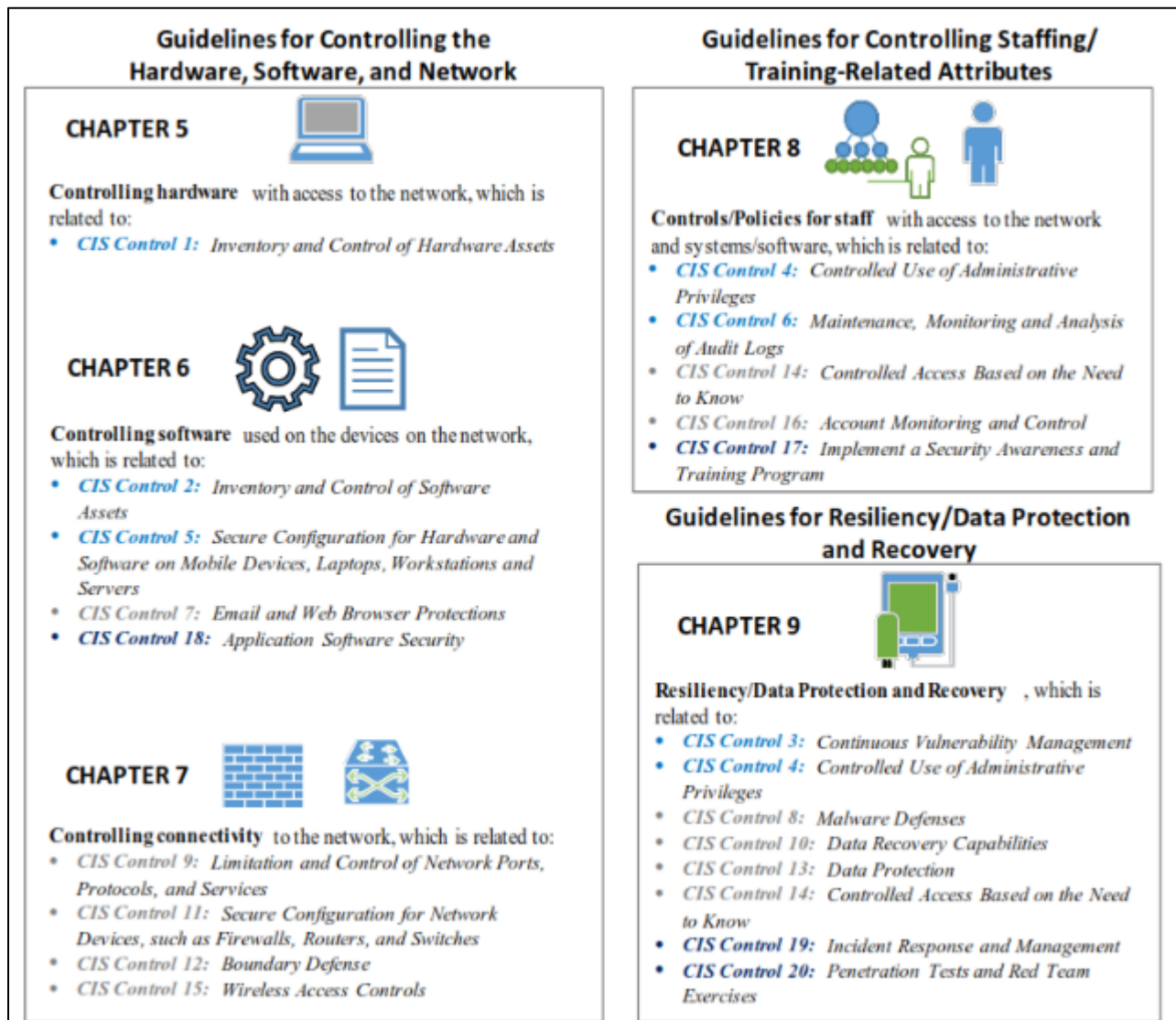


Figure 10: Center for Internet Security (CIS) Controls™

<sup>52</sup> <https://www.cisecurity.org/controls/cis-controls-list/>

- **TMC Best Practices** – The following practices were identified by agencies responding to a questionnaire completed by 17 TMCs around the country, coupled with review of reference literature:
  1. Using active and/or passive scanning tools to identify all devices attached to the network on a routine basis.
  2. Vendor-supported software residing on a demilitarized zone (DMZ) section of the network, so that remote support by Secure Sockets Layer (SSL) Virtual Private Network (VPN) access is only granted to the DMZ and not to the enterprise/business network.
  3. Using Access Control Lists (ACL) or equivalent network access techniques to limit outside access to specific machines or services, so that access is granted only to the devices/networks that need them or essentially managing the users/devices with a “need to know.”
  4. Requiring background checks for personnel that require access to control rooms, particularly with direct administrative/privileged access to software, systems, and data centers.
  5. Leveraging existing security policies governing the entire agency, not just the TMC.
  6. Updating cybersecurity policies at least once a year to fix anomalies in the procedures based on current trends.
  
- **Gaps/Areas of Improvement for TMCs** – The following were indicated as areas in need of improvement, per the scan of TMC operators and relevant literature:
  1. Network port security solutions, and the use of certificates to authenticate devices is not widely adopted.
  2. There does not appear to be widespread adoption of software/application whitelisting among TMC operators.
  3. The majority of TMC organizations have not performed a skills gap analysis to understanding the skills and behaviors of their workforce.
  4. The importance of patch management is not widely acknowledged.
  5. Multi-factor authentication is still lacking across many TMC systems.
  6. TMCs need to implement routine incident response exercises.
  7. There is an identified shortage of dedicated versus consolidated IT staff for TMCs.

- **Self-assessment Tool** – The report recommends the [DHS Cyber Resilience Review \(CRR\) process](#) to identify vulnerabilities and provides a sample cybersecurity resilience self-assessment tool in the appendix of the report.
- **Technical Guidelines and Recommended Practices** – The technical guidelines and recommended practices presented in the report are organized in three categories: 1) Controlling the Hardware, Software, and Network; 2) Controlling Staffing/Training-Related Attributes; and 3) Resiliency/Data Protection and Recovery. Figure 11 shows the relationship between CIS Controls™ and Traffic Management Center roles, along with corresponding chapters of the report that expand upon each set of guidelines.



**Figure 11: Center for CIS Controls™ and TMC roles, with Corresponding Chapters**  
 (Source: Transportation Management Center Information Technology Security report)

Selected highlights from the technical guidelines and recommended practices are noted in Table 6. For the comprehensive guidelines and practices, see Chapters 5-9 of the report.

**Table 6: Selected Highlights from Technical Guidelines**

Category and Related CIS Control(s)	Selected Highlights from Guidelines
<p><b>Controlling Hardware with Access to the Network (Chapter 5)</b></p> <p><u>Related to:</u></p> <ul style="list-style-type: none"> <li>– CIS Control 1: Inventory and Control of Hardware Assets</li> </ul>	<ul style="list-style-type: none"> <li>– Maintain a detailed asset inventory of devices connected to the network including device location, IP address, Media Access Control (MAC) address, and manufacturer name.</li> <li>– Implement device controls and firewalls.</li> <li>– Continually monitor what devices are connected to the network. Quarantine and/or remove unauthorized assets.</li> <li>– Use active asset management tools to scan the network, add and monitor for new devices, and flag them before granting access.</li> </ul>
<p><b>Controlling Software Used within the Network (Chapter 6)</b></p> <p><u>Related to:</u></p> <ul style="list-style-type: none"> <li>– CIS Control 2: Inventory and Control of Software Assets NIST RMF Identify</li> <li>– CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</li> <li>– CIS Control 7: Email and Web Browser Protections</li> <li>– CIS Control 18: Application Software Security</li> </ul>	<ul style="list-style-type: none"> <li>– Remove unnecessary software and separate high-risk applications from the most critical systems.</li> <li>– Track devices that have moved between networks in a test environment and a live-production environment and regularly check these devices for accuracy.</li> <li>– Monitor software applications on each computer and quarantine and/or remove unauthorized applications.</li> <li>– Ensure that only fully supported browsers and email clients are allowed on the network.</li> <li>– Evaluate, monitor, and correct exposure risks associated with application development and maintenance. For sensitive applications or data, encrypt the entire data flow using standardized encryption algorithms.</li> <li>– Consider risks and challenges of storing data in the cloud.</li> <li>– Select a cloud service model that balances control/integration flexibility and how much the agency can maintain/administer safely and securely.</li> </ul>
<p><b>Controlling Network Connectivity (Chapter 7)</b></p> <p><u>Related to:</u></p> <ul style="list-style-type: none"> <li>– CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services</li> <li>– CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches</li> <li>– CIS Control 12: Boundary Defense</li> </ul>	<ul style="list-style-type: none"> <li>– Strategically isolate critical infrastructure devices/systems to limit risk exposure.</li> <li>– Limit and control access to certain devices and network segments through port-filtering, a next-generation application firewall, client certificates; monitor unauthorized assets for removal or quarantine; and managing network devices using multi-factor authentication and encrypted sessions.</li> <li>– Identify/document the reasons why a configuration rule is in place to allow certain traffic to flow through the network.</li> <li>– Use detection and automated tools to compare network device configurations with known/approved configuration</li> </ul>

Category and Related CIS Control(s)	Selected Highlights from Guidelines
<ul style="list-style-type: none"> <li>– CIS Control 15: Wireless Access Controls</li> </ul>	<ul style="list-style-type: none"> <li>settings and to alert when deviations are found. Secure wireless LANs, access points, and end-user client systems. Enforce encryption of wireless data transmissions.</li> <li>– Create a separate wireless network for untrusted devices that are primarily granted access to the Internet but not the enterprise network.</li> </ul>
<p><b>Controlling Staffing/Training-related Attributes (Chapter 8)</b></p> <p><i>Related to:</i></p> <ul style="list-style-type: none"> <li>– CIS Control 4: Controlled Use of Administrative Privileges</li> <li>– CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs</li> <li>– CIS Control 14: Controlled Access Based on the Need to Know</li> <li>– CIS Control 16: Account Monitoring and Control</li> <li>– CIS Control 17: Implement a Security Awareness and Training Program</li> </ul>	<ul style="list-style-type: none"> <li>– In a larger organization, isolate who has access and authorization to make changes to systems and the network.</li> <li>– Control the use of administrative privileges and automated logging and monitoring.</li> <li>– Restrict what portions of the network and applications contract employees can access.</li> <li>– Scan ports for use of disabled and outdated credentials on a routine basis.</li> <li>– Raise employee awareness of cybersecurity and potential threats and offer related training.</li> <li>– Identify skill gaps and threat vectors requiring employee awareness, roll out training initiatives in a timely manner, and monitor compliance.</li> <li>– Remove account credentials from an employee at the time of their departure.</li> </ul>
<p><b>Improving Resiliency and Data Protection and Recovery of TMC IT and Operations (Chapter 9)</b></p> <p><i>Related to:</i></p> <ul style="list-style-type: none"> <li>– CIS Control 3: Continuous Vulnerability Management</li> <li>– CIS Control 4: Controlled Use of Administrative Privileges</li> <li>– CIS Control 8: Malware Defenses</li> <li>– CIS Control 10: Data Recovery Capabilities</li> <li>– CIS Control 13: Data Protection</li> <li>– CIS Control 14: Controlled Access Based on the Need to Know</li> <li>– CIS Control 19: Incident Response and Management</li> <li>– CIS Control 20: Penetration Tests and Red Team Exercises</li> </ul>	<ul style="list-style-type: none"> <li>– Partner within the agency or industry to share experiences and best practices for developing cybersecurity guidelines.</li> <li>– Utilize risk analysis to identify the greatest risks/weaknesses and employ a risk management plan.</li> <li>– Complete a risk assessment and develop a resiliency plan.</li> <li>– Develop an Incident Response Plan and execute periodic exercises to test the plan.</li> <li>– Determine the priority, scope, risk, and root cause of suspected incidents and identify the details of events.</li> <li>– Share lessons learned post-incident with all teams involved.</li> <li>– Monitor known sources of credible information about known threats and vulnerabilities.</li> <li>– Utilize centrally managed anti-malware software to defend each workstation/server.</li> <li>– Determine backup frequency, test backups for the existence of malware, maintain at least one backup offsite, and ensure higher recovery priority for data with higher impact.</li> <li>– Scrub personal information data from backups.</li> </ul>

## 7.2.2 Cybersecurity of Traffic Management Systems

The [NCHRP 03-127 Cybersecurity of Traffic Management Systems](#) project developed guidance for state and local transportation agencies to mitigate the risks from cyber-attacks on the field side of traffic management systems. The guidance addresses the vulnerability of field devices (e.g. traffic signal controllers and cabinets, dynamic message signs, Vehicle to Infrastructure (V2I) roadside units, weigh-in-motion systems, road-weather information systems, remote processing and sensing units, and other IP-addressable devices), field communications networks, and field-to-center communications. The guidance does not address vulnerabilities within a traffic management center, within center-to-center communications, or due to insider risk (accidental or intentional).

A web-based guidance tool hosted by the National Operations Center of Excellence (NOCoE) uses a risk-based decision tree to identify the most relevant content for a user. To use the [TRB Risk Assessment Web Guidance Tool](#),<sup>53</sup> individuals will first create a user account. The user is then led through a series of questions regarding their traffic management system field network. Upon completion of the questions, the user will receive a report with recommendations for cybersecurity improvements.

- **Devices** – The "devices" portion of the web tool will ask you to select from a list of devices used by your Transportation Management Center to determine if there any known vulnerabilities that pertain to those devices. See Figure 12.
- **Questions** – The "questions" portion of the web tool will ask a series of questions regarding different aspects of cybersecurity in relation to your Transportation Management Center. In total, there are approximately 102 questions. A page will display before the questionnaire to determine which types of questions you feel you are able to answer. Answering all questions for your selections should take around 10-15 minutes.
- **Results** – The "results" portion of the web tool will display recommendations based on information entered in the devices and questions portions. Your total scoring based on responses to questions through all the question types will be displayed as a chart alongside tables holding your responses and devices entered.

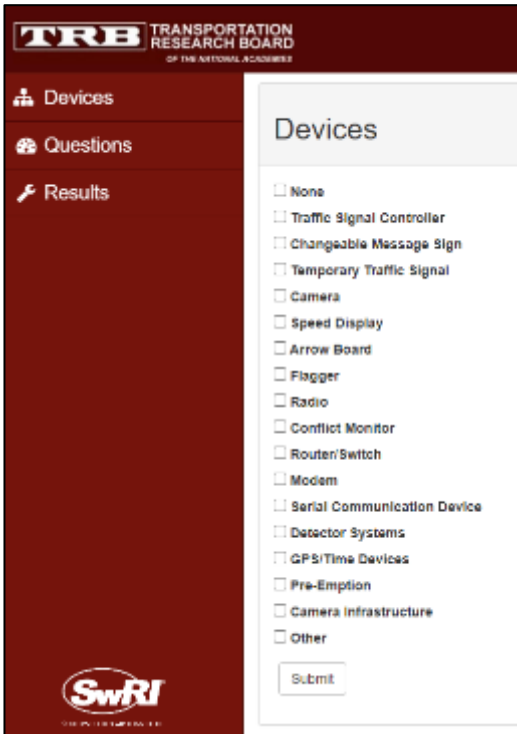
The screenshot shows a web interface for the TRB Risk Assessment Web Guidance Tool. The header includes the TRB logo and the text 'TRANSPORTATION RESEARCH BOARD OF THE NATIONAL ACADEMIES'. A dark red sidebar on the left contains three menu items: 'Devices' (selected), 'Questions', and 'Results'. The main content area is titled 'Devices' and features a list of checkboxes for various equipment types: None, Traffic Signal Controller, Changeable Message Sign, Temporary Traffic Signal, Camera, Speed Display, Arrow Board, Flagger, Radio, Conflict Monitor, Router/Switch, Modem, Serial Communication Device, Detector Systems, GPS/Time Devices, Pre-Emption, Camera Infrastructure, and Other. A 'Submit' button is located at the bottom right of the list. The SwRI logo is visible in the bottom left corner of the interface.

Figure 12: Screenshot Showing "Devices"

<sup>53</sup> <http://cyberguidance.transportationops.org>



- **Downloads** – Once you have completed the tool, a copy of your results will be available for download to easily load the next time you use the web tool.

A literature review [Cybersecurity Literature Review and Efforts Report](#) (Ramon and Zajac, 2018)<sup>54</sup> completed during the first task of NCHRP Project 03-127 served as a basis for developing the guidance. The literature review organizes resources such as relevant standards, capability models, and frameworks; relevant research; best practices and guidance from organizations such as DHS, the Transportation Research Board (TRB), American Public Transportation Association, and the USDOT National Highway Traffic Safety Administration; and related USDOT, state, and local programs.

---

<sup>54</sup> [http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127\\_Cybersecurity\\_Literature\\_Review.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127_Cybersecurity_Literature_Review.pdf)

## 8.0 Summary

---

This project utilized a “customer-centric” (i.e. agency-focused) approach to document emerging practices for ITS communications infrastructure. The research summarized agencies’ needs for long-distance data communications to field devices and related trends, options for long-distance communications with a focus on emerging technologies, and practices for managing communications infrastructure assets. The project conducted interviews with U.S. state and Canadian provincial transportation agencies, gathered input from commercial cellular service providers, and reviewed online resources and published literature to document current and emerging practices. This section presents an overview of selected key findings.

### **Emerging Needs for Long-Distance Data Communications**

- An analysis of emerging long-distance data communications needs identified trends such as potential increased use of “exception” communications through edge computing or ubiquitous data processing in the field rather than continuously communicating to a central location for data processing; a future that may require high bandwidth communications for CAV backhaul; and increased options for wireless communications services.

### **Current and Emerging Use of Cellular for Communications to Field Devices**

- Common uses for cellular service include low bandwidth field devices (e.g. DMS, weather stations, traffic signals), mobile devices to report road conditions and maintenance needs, and temporary devices such as portable traffic cameras or DMS used for work zones and special events.
- Cellular services generally meet agencies’ needs, especially where coverage is sufficient and low bandwidth devices are connected. However, cellular coverage can be limited in some rural areas, and performance lags at high use sites (e.g. near a stadium) or can be insufficient during high use periods (e.g. evacuations) with heavy vehicle traffic and cellular phone use.
- 5G cellular service, FirstNet, and LPWAN are emerging options for data communications to field devices. Though 5G may not be used for long-distance field device communications in the near future, it has gained attention due to its expected high-speed, low latency data transfer capabilities. FirstNet offers dedicated communications for emergency responders and supporting entities (e.g. transportation agencies), presenting a new option for ITS field device communications. LPWAN can offer lower rate plans for low-bandwidth field device applications.

#### **Primary factors for selecting field device communications:**

- Availability/Coverage
- Bandwidth Needs
- Cost
- Security
- Reliability

#### **Selecting Communications Infrastructure:**

- Primary factors for selecting field device communications include availability/coverage, device bandwidth needs, cost, security, and reliability. Many agencies noted that availability/coverage and bandwidth needs were the top two considerations. Though cost is a consideration, agencies are often bound by the type of infrastructure or services available at the site.

- Some agencies are implementing or exploring edge computing solutions and cloud computing services to move complex data processing to the field or to the cloud. These strategies can simplify operations and condense large datasets to alleviate centrally located data storage needs. Edge or cloud computing can also reduce the need for continuous communications to transfer data back to a central site, conserving bandwidth and making a wider range of communications options available.
- Most agencies that are deploying connected vehicle (CV) applications indicated that time-critical data processing occurs in the field, and data transfers (primarily for health monitoring and device updates) are limited to low volumes of data to and from a central site. Most agencies use fiber for CV backhaul, with cellular used where fiber is not available. Most agencies indicated that their current and planned communications infrastructure will be sufficient to meet CV backhaul needs.

### Long-term Management Practices:

- A 2019 FCC rulemaking that establishes shot clocks for agency review and approval of requests to install small wireless facilities (i.e. 5G small cells) on public rights-of-way has prompted agencies to develop related policies and procedures. Many agencies indicate a preference or even a requirement for small cell installations to be on newly constructed structures/poles, due to concerns (e.g. safety, structural capacity) about mounting equipment on in-place DOT structures.
- DOT practices for allowing right-of-way access to telecommunications providers tend to be driven by initiatives that encourage broadband development and leverage resources statewide.
- Several transportation agencies allow non-DOT entities to co-locate equipment (e.g. transceivers) on DOT-owned towers. Some agencies only allow access to other government entities while others allow private sector entities to co-locate, and fees vary by agency.
- Some agencies are successful in accessing communications assets and services through sharing arrangements with the private sector, including fiber sharing, resource trading, and public-private partnerships. The allowance of such arrangements is often governed by state law, and when allowed, can leverage public and private resources for mutual benefit of all parties involved.
- Agencies that track fiber locations and attributes may use in-house tools (e.g. spreadsheets, databases, mapping tools) or off-the-shelf products. Agencies that systematically track fiber networks often utilize geographic information system (GIS) tools to display related information.
- In terms of managing communications infrastructure-related licenses and agreements, practices vary by agency. However, agencies typically assign dedicated staff to obtain and manage FCC licenses, such as monitoring renewal timelines and other license details. Co-location

An FCC rulemaking that establishes shot clocks for review and approval of requests to install small wireless facilities (i.e. 5G small cells) on public rights-of-way has prompted agencies to develop related policies and procedures.

arrangements are documented in formal agreements and details are tracked internally within the agency.

**Security:**

- Physical security of field boxes, shelters, and cabinets is critical to protect equipment from vandalism and security breaches. Common tactics include changing out standard/universal keys, electronic lock systems, multiple locks, and modifications to equipment placement (e.g. burying underground or high mounting).
- Security at DOT communications facilities such as radio towers and tower buildings can be accomplished through alarms, dual locks, real-time access verification and entry/exit logs for staff and co-locating entities, and pre-established clearance checks.
- General cybersecurity practices include ensuring current software patches, removing factory default passwords from field devices, VPNs for cellular communications, and ITS networks that are not connected to the internet.
- Security for connected vehicle deployments often involves multiple strategies to secure RSUs in the field to mitigate hacking into DOT networks. This includes limiting access to RSUs with only authenticated devices and using VPNs and built-in firewalls when cellular modems are used.

## Appendix A: Input from Transportation Agencies

---

- California Department of Transportation (Caltrans)
- Florida Department of Transportation (FDOT)
- Georgia Department of Transportation (GDOT)
- Michigan Department of Transportation (MDOT)
- Minnesota Department of Transportation (MnDOT)
- New Hampshire Department of Transportation (NHDOT)
- North Dakota Department of Transportation (NDDOT)
- Ontario Ministry of Transportation (MTO)
- Utah Department of Transportation (UDOT)
- Wisconsin Department of Transportation (WisDOT)

## Emerging Practices for Communications Infrastructure

### Interview Summary

California Department of Transportation (Caltrans)

<b>Interview Date and Participant</b>	February 20, 2020 - Phone interview with Ferdinand Milanes, Caltrans
<b>Current Use of Cellular Services for Long-Distance Communications</b>	<p><b>Current Cellular Use:</b></p> <ul style="list-style-type: none"> <li>• Low bandwidth cellular is used for less intensive field device applications such as controlling Highway Advisory Radio (HAR), Dynamic Message Signs (DMS), road weather systems, and ramp meters. Caltrans is also using cellular service to communicate with mobile devices used by maintenance staff to report road conditions and maintenance needs.</li> <li>• Caltrans has a statewide contract with Verizon. In some areas where Verizon services are limited, other providers are utilized (e.g. AT&amp;T, mountain cellular).</li> <li>• 3G, 4G, 4G LTE, and analog service are used by Caltrans.</li> <li>• Cellular services are procured from providers.</li> <li>• Caltrans needs are being met by cellular for low bandwidth applications. However, there is a need for additional coverage/service in some areas of the state, especially in rural areas.</li> </ul> <p><b>Cost for Cellular Service:</b></p> <ul style="list-style-type: none"> <li>• The cost for cellular service tends to be slightly higher in rural areas, as the cost to bring service to these less populated areas may be higher for providers. But the costs are dependent on many factors (e.g. number of devices, usage).</li> <li>• Caltrans typically tries to procure unlimited data plans.</li> <li>• Caltrans has commissioned a study that includes a communications cost component; results of this study can be shared when available.</li> <li>• The cost for cellular service on FirstNet (nationwide public safety broadband network) is \$37.99/device per month with unlimited data in District 4 which is the San Francisco Bay Area.</li> </ul>
<b>Emerging Use of Cellular Services for Long-Distance Communications</b>	<p><b>Emerging Cellular Services:</b></p> <ul style="list-style-type: none"> <li>• The buildout of FirstNet offers a new opportunity for expanded cellular coverage and to co-locate on radio facilities, to serve multiple needs.</li> </ul> <p><b>Permitting Small Cell Installations in Agency-Owned Right-of-Way (ROW):</b></p> <ul style="list-style-type: none"> <li>• Caltrans has established a committee to address provider requests for 5G small cell installations on the ROW. There has not been any 5G equipment installed to date.</li> <li>• Caltrans has a wireless licensing agreement and process to utilize for 5G co-location requests: <a href="https://dot.ca.gov/programs/right-of-way/wireless-licensing-program">https://dot.ca.gov/programs/right-of-way/wireless-licensing-program</a></li> </ul>

<p><b>Selecting Communications Infrastructure</b></p>	<p><b>Selection Considerations:</b></p> <ul style="list-style-type: none"> <li>• In many cases, Caltrans selects communications mechanisms and providers based on available coverage and bandwidth needs. Caltrans pays for services needed (e.g. mountaintop coverage) and cannot control resulting costs if there is only one provider with service at a location, for example.</li> <li>• Although cost comparisons on all communications options are considered, the first choice is to utilize Caltrans-owned facilities; the second choice is to co-locate with other state, city, or county owned facilities (or to procure services from private providers); and the last option is to build new infrastructure.</li> <li>• Cellular can be the most economical choice in some cases. If capacity and bandwidth needs are met, use of procured services eliminates the need for agency-performed maintenance.</li> <li>• Caltrans will typically install fiber or empty conduit in their own ROW when a major road construction project occurs. There is a high cost associated with installing fiber at locations not within Caltrans ROW, due the need to obtain permits and environmental clearances.</li> <li>• All Caltrans capital projects have a broadband component included in the planning documents. This was instituted to “bridge the digital divide” by allowing broadband providers to co-locate in DOT facilities, but it has also helped to ensure that the necessary communications components aren’t inadvertently omitted from project designs.</li> </ul> <p><b>Exception Communications and Developments in Computing Topology:</b></p> <ul style="list-style-type: none"> <li>• Caltrans does not utilize cloud-based computing. Field devices are connected to the Transportation Management Center (TMC) where the data from field devices is sent and processed.</li> </ul> <p><b>Current Backhaul and Future CAV Backhaul Needs:</b></p> <ul style="list-style-type: none"> <li>• Fiber is used mostly for backhaul communications, and high bandwidth applications (CCTV). Caltrans will lease a fiber line or utilize Caltrans-owned fiber from the TMC to a hub, which connects to other mechanisms communicating to field devices. In some cases, end to end fiber is used. Fiber is used more for high bandwidth uses such as cameras.</li> <li>• Caltrans is also licensing in the 4.9 MHz band for backhaul, however it is unclear if this is still a good option with a potential FCC ruling that may reduce available spectrum in this band.</li> <li>• FirstNet could also be an option to consider for backhaul, with higher capacity that is dedicated for public safety users.</li> </ul> <p><b>Maintenance/Other:</b></p> <ul style="list-style-type: none"> <li>• A significant challenge with DOT-owned communications facilities is a shortage of staff with expertise to maintain these assets.</li> </ul>
<p><b>Long-Term Management Practices</b></p>	<p><b>Right-of-Way Access for Broadband Providers:</b></p> <ul style="list-style-type: none"> <li>• In the early 1990s’s, Caltrans developed a master license agreement to allow cellular providers to lease space in Caltrans ROW, with an associated cost: <a href="https://dot.ca.gov/programs/right-of-way/wireless-licensing-program">https://dot.ca.gov/programs/right-of-way/wireless-licensing-program</a></li> <li>• More recent California legislation allows broadband providers to install fiber or empty conduit in the right-of-way when Caltrans is doing highway work. A user guide outlines processes to facilitate broadband conduit installation:</li> </ul>

	<p><a href="https://dot.ca.gov/-/media/dot-media/programs/design/documents/wired-broadband-facility-user-guide--1-01_edition-a11y.pdf">https://dot.ca.gov/-/media/dot-media/programs/design/documents/wired-broadband-facility-user-guide--1-01_edition-a11y.pdf</a>.</p> <ul style="list-style-type: none"> <li>• Caltrans maintains a web page for broadband providers to view upcoming projects: <a href="https://dot.ca.gov/programs/design/wired-broadband">https://dot.ca.gov/programs/design/wired-broadband</a>.</li> <li>• Caltrans also offers private providers to co-locate on DOT-owned radio facilities, such as vaults and towers.</li> </ul> <p><b>Resource Sharing:</b></p> <ul style="list-style-type: none"> <li>• Caltrans does not share DOT-owned fiber.</li> </ul> <p><b>Tracking Assets:</b></p> <ul style="list-style-type: none"> <li>• Each district tracks their fiber assets using geographic information system (GIS) tools.</li> <li>• Each co-location on DOT-owned radio facilities is tracked and contains details such as the provider information and type of equipment.</li> <li>• All cellular co-locations on DOT facilities are also tracked via site license agreements.</li> <li>• The California Office of Emergency Services tracks all FCC licenses statewide. At Caltrans, FCC licenses are tracked in a database and in a physical file for each license.</li> </ul>
<b>Security</b>	<p><b>Physical Security:</b></p> <ul style="list-style-type: none"> <li>• Radio sites (transmitters and receivers) are increasingly being placed along the highway which has led to an increase in vandalism.</li> <li>• Copper wire has been changed to aluminum wire, due to copper wire theft.</li> <li>• Pull boxes are buried deeper to decrease instances of vandalism. <ul style="list-style-type: none"> <li>– Caltrans standard specifications for Pull Boxes (86-1.02C) and Installation of Pull boxes (Sect 87-103C): <a href="https://dot.ca.gov/programs/design/ccs-standard-plans-and-standard-specifications">https://dot.ca.gov/programs/design/ccs-standard-plans-and-standard-specifications</a></li> </ul> </li> <li>• An alarm alerts the statewide operations center when a door is opened at a radio tower, allowing those entering and exiting to identify themselves and to log entries and exits to the tower.</li> <li>• Caltrans radio coordinators typically accompany individuals from co-locating entities that request access to DOT-owned radio towers.</li> </ul> <p><b>Cybersecurity:</b></p> <ul style="list-style-type: none"> <li>• Fiber is one of the most secure communication mechanisms because it's located underground. Radio and cellular are not as secure as fiber.</li> </ul>



## Emerging Practices for Communications Infrastructure

### Interview Summary

Florida Department of Transportation (FDOT)

<b>Information Source</b>	February 20, 2020 written response to interview question guide from Randy Pierce, FDOT (Note: This summary also includes information from FDOT’s website as noted.)
<b>Current Use of Cellular for Long-Distance Communications</b>	<ul style="list-style-type: none"> <li>• Florida does not consider cellular as a Public Safety provider, and as such these systems are not typically procured in meeting FDOT’s needs.</li> <li>• FDOT’s Planning group has utilized cellular systems for road-counts for arterials and interstates.</li> <li>• With limitations demonstrated in the cellular industry with maintaining critical communications needs during major outages, FDOT maintains its own Land Mobile Radio system. This network provides continuous state-wide coverage if required or day-to-day within the Districts. Connectivity of this network is provided via the ITS network.</li> </ul>
<b>Emerging Use of Cellular Services for Long-Distance Communications</b>	<p><b>Emerging Cellular Services:</b></p> <ul style="list-style-type: none"> <li>• AT&amp;T (First Net) has approached several FDOT Districts with discussions around Multilink in providing communications with Florida’s Road Rangers Service Patrol programs. FDOT has not pursued this option.</li> </ul>
<b>Selecting Communications Infrastructure</b>	<p><b>Selection Considerations and Current Buildout:</b></p> <ul style="list-style-type: none"> <li>• FDOT applies selection of communications infrastructure on a case-by-case basis, primarily considering whether it is critical or need to know data.</li> <li>• FDOT will continue to support its owned communications system.</li> <li>• Cellular is typically not procured by FDOT, as it has not demonstrated reliability during critical needs.</li> <li>• FDOT is currently in a multiphase procurement process that will upgrade the older Motorist Aid Call Box system infrastructures with current technologies in switches, routers and associated equipment. This will include an upgrade to the existing microwave system from a 48 MGP/s to a 400 MGP/s network throughout the state. These systems are designed with 99.999% reliability with emergency backup gen-sets and 48Volt DC battery plants providing ITS critical infrastructure needs.</li> <li>• FDOT is currently expanding their fiber networks along the Limited Access Right-of Way utilizing a Multiprotocol Label Switching (MPLS) infrastructure, coupled with a microwave buildout.</li> </ul> <p><b>Current Backhaul and Future CAV Backhaul Needs:</b></p> <ul style="list-style-type: none"> <li>• FDOT’s ITS infrastructure can meet the capabilities as needed. As ITS communications continue to place demands on FDOT’s infrastructures it remains critical to expand FDOT systems’ capabilities to meet these needs. As such, FDOT sees no issues with completing their communications infrastructure buildout as needed.</li> </ul>

<p><b>Long-Term Management Practices</b></p>	<p><b>Co-Location Agreement with Wireless Providers:</b></p> <ul style="list-style-type: none"> <li>• Under the Telecommunications Act, Florida DOT entered into a contract with American Tower known as Lodestar.</li> <li>• This agreement with Lodestar provides exclusive rights to market and sublease space on certain FDOT towers. With this agreement, Lodestar may enter into sublease agreements with wireless providers while providing FDOT with a percentage of the gross receipts derived from these subleases. This strategy encourages wireless service providers to co-locate on towers located primarily on FDOT's limited-access rights-of-way rather than developing numerous new tower sites in local communities. Information on Lodestar: <a href="http://www.fdot.gov/traffic/its/projects-telecom/lodestar.shtm">www.fdot.gov/traffic/its/projects-telecom/lodestar.shtm</a>.</li> </ul> <p><b>Fiber Tracking:</b></p> <ul style="list-style-type: none"> <li>• FDOT has been working with Byers Engineering, <a href="http://nexusworx.byers.com/">NexusWorx™</a> Fiber ITS Asset Management since 2006. (See <a href="http://nexusworx.byers.com/">http://nexusworx.byers.com/</a>) Known as ITS Facilities Management (ITSFM), the system provides specific requirements within the FDOT ITS infrastructure as built documentation.</li> <li>• The <a href="#">FDOT ITSFM</a> is an asset, configuration, and document management system that compiles assets information into a single, accessible GIS based graphical and tabular database. The ITSFM web-based application provides for the modeling of the fiber network facilities and connected fiber devices, as well as ITS devices and the electrical system powering the ITS device sites.</li> <li>• Information about FDOT's ITSFM: <a href="http://www.fdot.gov/traffic/itsfm/newusersagencies/about-itsfm">www.fdot.gov/traffic/itsfm/newusersagencies/about-itsfm</a></li> </ul> <p><b>Managing FCC Licenses:</b></p> <ul style="list-style-type: none"> <li>• FCC licensing is verified and/or maintained via the Central Office TSM&amp;O under a scope of work issued to FDOT's Telecommunications General Consultant contractor.</li> </ul>
<p><b>Security</b></p>	<ul style="list-style-type: none"> <li>• FDOT's ITS network is built out as "intranet" and has no internet connectivity.</li> <li>• Access into facilities requires Department of Homeland Security (DHS) Level 2 / Criminal Justice Information Services clearances for all personnel.</li> <li>• All third-party leases are required to have their own shelter and electrical power on co-located tower sites. State, City and/or County Public Safety co-locates are provided with access under FDOT's Tower/Shelter Use Agreements under the same security requirements.</li> </ul>
<p><b>Other Emerging Communications Mechanisms</b></p>	<ul style="list-style-type: none"> <li>• FDOT has established a memorandum of understanding with the National Oceanic and Atmospheric Administration (NOAA) with access from the <a href="#">Geostationary Operational Environmental Satellite (GOES)</a> system. These deployments have provided FDOT with "0" monthly communications costs associated with Road Weather Information Systems (RWIS) stations currently deployed on bridges. A high level of reliability is achieved with two satellite-to-ground stations that are directly coupled with the FDOT ITS network.</li> </ul>

## Emerging Practices for Communications Infrastructure

### Interview Summary

Georgia Department of Transportation (GDOT)

<b>Interview Date and Participant(s)</b>	June 10, 2020 – Phone interview with John Hibbard and Alan Davis, GDOT
<b>Selecting Communications Infrastructure</b>	<p><b>Selecting Communications Infrastructure:</b></p> <ul style="list-style-type: none"> <li>• Use of fiber to communicate to field devices: <ul style="list-style-type: none"> <li>– Performance of fiber is excellent, in terms of bandwidth and reliability.</li> <li>– Agency-owned fiber includes the flexibility to make changes as needed.</li> <li>– Maintenance can be a challenge with owned fiber. The agency needs to locate, protect, and repair fiber lines when damage occurs (e.g. due to digging activities). The agency’s IT department needs to be well-prepared to deal with a large network of fiber and devices.</li> </ul> </li> <li>• Use of cellular to communicate to field devices: <ul style="list-style-type: none"> <li>– Use of cellular is determined on a case-by-case basis, depending on functional needs and whether a fiber connection is available.</li> <li>– Cellular can be the most economical choice (compared to installing fiber) for lower bandwidth applications, such as connecting to signals statewide. However, cellular does carry a significant ongoing operations cost due to continuous service fees.</li> <li>– Bandwidth and latency of cellular is adequate for communicating to devices like signals and dynamic message signs, where low volumes of data are transferred. However, when adding other field devices (e.g. cameras, roadside units) to a network, cellular is not the preferred option due to higher bandwidth needs overall.</li> </ul> </li> <li>• Emerging cellular: <ul style="list-style-type: none"> <li>– Currently, the buildout of 5G cellular is concentrated in urban areas.</li> </ul> </li> </ul>
<b>Connected Vehicle (CV) Backhaul</b>	<p><b>Urban CV Deployments:</b></p> <ul style="list-style-type: none"> <li>• GDOT has deployed more than 600 roadside units (RSUs) in the Atlanta metro area. All RSUs communicate SPaT and MAP data, with some deployments for transit signal priority and emergency vehicle preemption.</li> <li>• Data processing occurs locally at the intersection (i.e. at the edge).</li> <li>• The vast majority of RSUs are connected to fiber for backhaul. A few are connected to cellular where fiber is not available.</li> <li>• Data transfers to RSUs from a central location and vice versa are limited to low volumes of data for remote monitoring, management, and RSU updates.</li> <li>• GDOT has conducted demonstrations where large CV datasets were communicated from RSUs to the DOT via fiber. <ul style="list-style-type: none"> <li>– Fiber backhaul was adequate for these large volume data transfers.</li> <li>– Due to a concern about storage capacity for large CV datasets, GDOT is exploring edge computing solutions and/or increased processing capabilities at a central location.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• GDOT conducted a test in which SPaT and MAP data was streamed through the internet using cellular, to test latency and bandwidth capabilities. Cellular performed well, due to a strong LTE cellular network in the Atlanta area and relatively small volumes of data being communicated.</li> </ul> <p><b>Rural CV Deployment:</b></p> <ul style="list-style-type: none"> <li>• A new deployment, in partnership with Panasonic, will soon be operational to test CV applications such as queue warning and weather incident warning.</li> <li>• Includes 6 RSUs on rural I-85, with a limited number of equipped vehicles.</li> <li>• Data processing occurs at the roadside for time-critical applications.</li> <li>• Data is also communicated from the roadside to Panasonic’s cloud datacenter for processing and analytics. Static and dynamic data messages are sent from the Panasonic centralized platform back to the roadside.</li> <li>• 4G cellular will be used for long-distance backhaul communications, as fiber is not available in the area.</li> <li>• Though the deployment is not fully operational, initial testing of cellular for long-distance data communications was successful. Cellular coverage in that area is good, and low volumes of data are being transferred.</li> </ul> <p><b>Security:</b></p> <ul style="list-style-type: none"> <li>• Physical security measures include monitoring access to field devices, to ensure proper credentials by staff when accessing field devices that are connected to the ITS network.</li> <li>• For RSUs connected to cellular for backhaul, a secure tunnel within the cellular provider’s network provides a private connection for long-distance data transfers.</li> <li>• Security credentialing (SCMS) is used to verify CV messaging (i.e. basic safety messages). The rural deployment is using SCMS, and GDOT will soon establish SCMS for the urban deployments.</li> </ul>
<p><b>Communications Infrastructure Planning</b></p>	<p><b>Plans for Statewide Fiber Network:</b></p> <ul style="list-style-type: none"> <li>• GDOT’s fiber network is 100% agency owned and located in the Atlanta area.</li> <li>• GDOT is in the process of planning for a statewide fiber network. The overall goal of this effort is to establish reliable connections to ITS devices statewide.</li> <li>• A driving factor for this initiative was an evacuation event that produced heavy traffic on I-95 in southern Georgia during a hurricane event in Florida. <ul style="list-style-type: none"> <li>– During this event, the cellular network was overloaded due to heavy vehicle traffic and cellular phone use, and GDOT’s ability to connect to ITS devices via cellular was severely compromised. It is unlikely that the cellular network will be expanded to cover communications needs in such a rare event.</li> <li>– GDOT determined a need for improved reliability during critical events.</li> </ul> </li> <li>• GDOT is aiming to establish a public-private partnership (P3) model for broadband development, with a goal of establishing a combination of agency-owned and privately owned fiber along the interstates.</li> <li>• Expansion of DOT-owned fiber backbone is underway with installation of fiber along I-95, and the agency continues to search for P3 partnerships.</li> </ul> <p><b>Fiber Tracking:</b></p> <ul style="list-style-type: none"> <li>• GDOT uses NexusWorx for tracking fiber. See: <a href="http://nexusworx.byers.com/">http://nexusworx.byers.com/</a></li> </ul>

## Emerging Practices for Communications Infrastructure

### Interview Summary

#### Michigan Department of Transportation (MDOT)

<b>Interview Date and Participant(s)</b>	April 22, 2020 – Phone interview with Jim Tamarelli, Michigan Department of Technology, Management and Budget (MDOT ITS Program Office)
<b>Current Use of Cellular Services</b>	<ul style="list-style-type: none"> <li>• Approximately 350 traffic control and monitoring field devices (e.g. cameras, detectors, DMS) are connected via cellular service. Weather stations and mobile snowplow operations also utilize cellular.</li> <li>• The state is currently updating 3000 traffic signals statewide which will be on cellular modems.</li> <li>• Most devices in rural areas are on 3G where fiber is not available.</li> <li>• Michigan has a statewide contract with Verizon.</li> <li>• Cellular modems are currently on public IPs, but these will soon be moved to private IPs with Verizon to increase security.</li> <li>• The performance of cellular is meeting MDOT’s needs for communicating to field devices. It is reliable and provides sufficient bandwidth.</li> </ul>
<b>Selecting Communications Infrastructure</b>	<ul style="list-style-type: none"> <li>• Michigan owns approximately 500-700 miles of fiber, exclusively in urban areas (e.g. Detroit, Grand Rapids) along interstates. A radio network is in place from Bay City to Flint along I-75 and in the Lansing area on I-96 &amp; I-496.</li> <li>• Cable modems are used for some devices at locations where service is available. For example, all 200 devices, some with low bandwidth needs, on MDOT’s US-23 Flex Route lane control system are on cable modems that are connected to fiber for last-mile communication.</li> <li>• Though fiber is preferred for communicating to field devices, it is expensive to install and to lease. Therefore, cellular can be an economical option where fiber is not available.</li> <li>• The state has explored leasing or sharing arrangements for fiber use, but barriers include:             <ul style="list-style-type: none"> <li>– The state cannot share fiber with for-profit entities without approval by the legislature.</li> <li>– Agreements with fiber providers do not include an option to exchange non-monetary goods/services for fiber use.</li> <li>– Cost sharing with the city of Grand Rapids school system has been utilized, but these types of arrangements are not common.</li> </ul> </li> </ul>
<b>CAV Backhaul</b>	<ul style="list-style-type: none"> <li>• MDOT has deployed approximately 400 roadside units (RSUs) in the in tri-county Detroit area.</li> <li>• 95% of the RSUs and related devices (e.g. cameras, detectors) are connected to fiber for data backhaul; one corridor is on cellular.</li> <li>• A typical connected vehicle (CV) site communicates 3-4 MB per second and is currently accessed/viewed by a central site for brief periods of time.</li> </ul>

	<ul style="list-style-type: none"><li>• The current backhaul infrastructure is sufficient for this volume of data transfer; however, the amount of data transferred for CV applications may increase over time.</li><li>• There is a concern that RSU sites which broadcast wirelessly could be hacked, potentially exposing the statewide communications network to security vulnerabilities. MDOT is exploring security mitigation measures at the server end of CV communications.</li><li>• There are no current plans to change or expand communications infrastructure to accommodate CV backhaul. The next urban area to have CV deployments will be Grand Rapids, which has a fiber network in place for backhaul.</li></ul>
--	--

## Emerging Practices for Communications Infrastructure

### Interview Summary

#### Minnesota Department of Transportation (MnDOT)

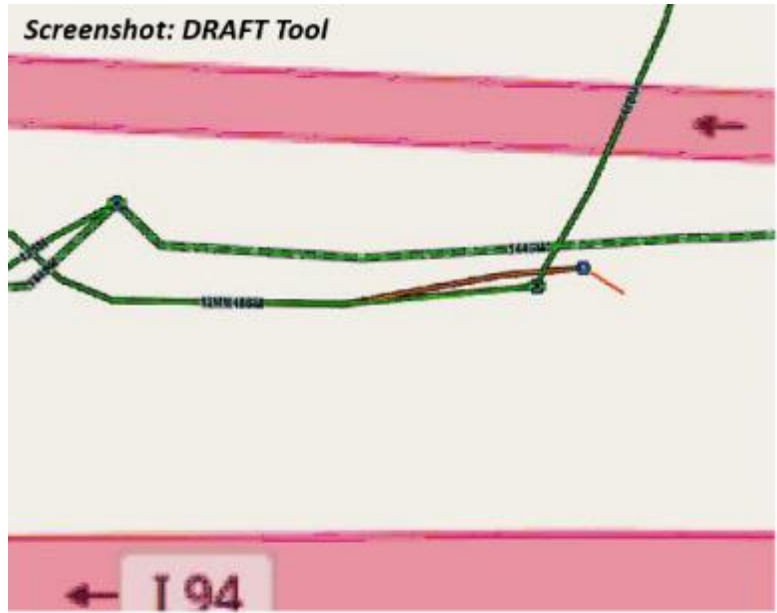
<b>Interview Date and Participants</b>	April 30, 2020 - Phone interview with Ralph Adair, Terry Haukom, Jim Mohn, Tim Lee, and Shane Chatleain (MnDOT)
<b>Current Use of Cellular for Long-Distance Data Communications</b>	<p><b>Current Cellular Use:</b></p> <ul style="list-style-type: none"> <li>• Cellular service is used where reasonable access to a physical connection (e.g. fiber, DSL, cable) is not available. <ul style="list-style-type: none"> <li>– Cellular is used mostly for low-bandwidth applications such as portable DMS and RWIS stations.</li> <li>– Cellular is used for high bandwidth applications (e.g. cameras) if needed, but performance lags.</li> <li>– Primarily using 4G LTE service.</li> <li>– Most field devices are on a Virtual Private Network (VPN) with Verizon.</li> </ul> </li> <li>• Some issues with cellular in rural areas with limited coverage, and for temporary devices located near intermittent high load sites like a stadium.</li> <li>• Troubleshooting issues can be difficult with third party services. It typically takes more staff time and visits to the site to resolve an issue.</li> </ul> <p><b>Cellular Costs:</b></p> <ul style="list-style-type: none"> <li>• Initial capital cost is approximately \$800, for the modem and antenna.</li> <li>• Operating cost varies from \$5-\$35/month, plus monthly usage fees.</li> </ul>
<b>Emerging Use of Cellular for Long-Distance Data Communications</b>	<p><b>Emerging Cellular Services:</b></p> <ul style="list-style-type: none"> <li>• No field devices are currently connected to 5G. 5G ruggedized (i.e. built for outdoors) modems are not widely available.</li> <li>• MnDOT is now on a public safety plan contract with Verizon.</li> </ul>
<b>Selecting Communications to Field Devices</b>	<p><b>Selection Considerations:</b></p> <ul style="list-style-type: none"> <li>• Selection of communications infrastructure is site-specific and chosen primarily based on available infrastructure (e.g. state-owned fiber) or service (e.g. cellular, microwave) at the site of the field device deployment.</li> <li>• Other considerations include bandwidth needs and cost.</li> <li>• Capital funding is easier to obtain than operating funds: <ul style="list-style-type: none"> <li>– It is generally more practical to build and own fiber using capital funds.</li> <li>– Long-term operating costs for cellular or leased fiber can be expensive, and operating funds to pay ongoing fees are more difficult to secure.</li> <li>– An added benefit with building fiber is providing service to state-owned buildings such as truck stations in addition to field devices, leveraging the capital investment for multiple purposes.</li> </ul> </li> </ul> <p><b>Edge Computing and Exception Communications:</b></p> <ul style="list-style-type: none"> <li>• Edge computing is used at a pump station that continuously monitors conditions for flooding. The system communicates by exception to notify</li> </ul>

	<p>MnDOT dispatch when flooding occurs. MnDOT also periodically accesses data from the pump station to assess system performance and create reports.</p> <ul style="list-style-type: none"> <li>• MnDOT is investigating other options for edge computing applications: <ul style="list-style-type: none"> <li>– <i>Tolling enforcement</i>: Use of field/edge computing for this application is driven by a need to quickly process a visual record of offenders on-site.</li> <li>– <i>Connected and Automated Vehicle (CAV) data management</i>: CAV applications will generate large volumes of data that can be processed in the field to produce smaller, more manageable datasets that are transferred back to a central location such as a TMC. Agencies can create rules to report only the CAV data they find useful and want to receive, rather than communicating all CAV data from the field. Processing at the edge also offers a security advantage; nominalizing these CAV datasets helps with data privacy by making the data less trackable.</li> </ul> </li> </ul> <p><b>Preparing for CAV Backhaul</b></p> <ul style="list-style-type: none"> <li>• MnDOT is conducting a study to assess bandwidth capacity statewide and developing a tool to track current and future communications needs and capacity, including for CAV data backhaul.</li> <li>• Performing CAV data processing in the field (edge computing) will reduce the volume of data communicated via backhaul, conserving bandwidth and enhancing data privacy.</li> </ul>
<p><b>Long-Term Management Practices</b></p>	<p><b>Access to Space on MnDOT-owned Towers</b></p> <ul style="list-style-type: none"> <li>• MnDOT owns, builds, operates, and maintains the Allied Radio Matrix for Emergency Response (ARMER), Minnesota’s shared public safety radio communication system.</li> <li>• Cities, counties, and other public safety or governmental agencies can request to use space on towers and shelters where there is excess capacity. Other wireless users (non-public safety and private) may also request to use capacity on towers where the capacity is not required for public safety users.</li> <li>• A fee is assessed for private entities’ use of MnDOT tower space. Public safety entities are not assessed a fee for occupying space, but a nominal charge for power/electricity consumption is collected.</li> <li>• Related procedures: <a href="http://www.dot.state.mn.us/oec/pdf/procedures.pdf">http://www.dot.state.mn.us/oec/pdf/procedures.pdf</a></li> </ul> <p><b>Fiber Sharing:</b></p> <ul style="list-style-type: none"> <li>• MnDOT shares fiber with another state agency (Minnesota IT Services) which exists to provide connectivity to state, county, and city entities.</li> <li>• MnDOT generally shares dark fiber with very clear lines of responsibility established, which limits security concerns.</li> </ul> <p><b>Fiber Tracking:</b></p> <ul style="list-style-type: none"> <li>• MnDOT currently uses GIS for location tracking and MicroStation CAD software for individual strand management.</li> <li>• MnDOT is building an in-house visual tool (80% complete) for strand management that combines its fiber management database with GIS location information. The following images show screenshots from the draft tool.</li> </ul>

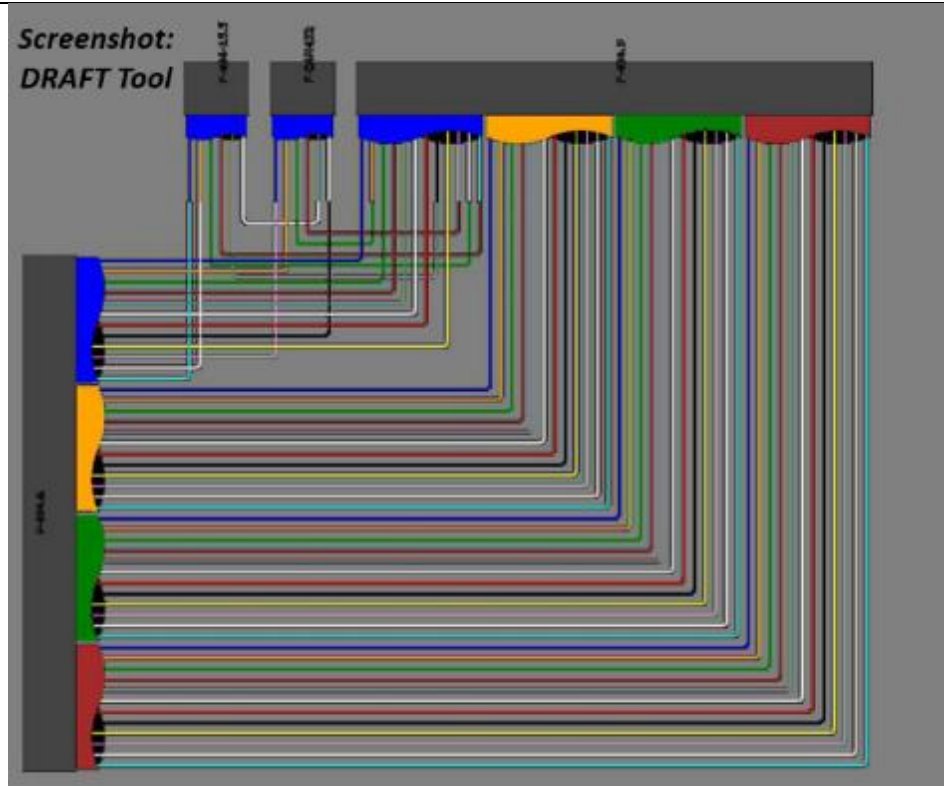




Map showing fiber splice enclosures on fiber system



Closer view of splice enclosure



*Visual diagram based on a database of the strand connectivity*

**Managing Tower Space Leases and FCC Licenses:**

- MnDOT tracks tower space leases through formal agreements in MnDOT’s document management system. Locations are tracked in a database and in as-builts.
- The MnDOT Office of Statewide Radio Communications’ engineering group obtains and manages FCC licenses. Staff actively monitor licenses for renewals and utilize the FCC’s database and related notifications to manage licenses.

**Physical Security**

- Radio tower security:
  - Staff in MnDOT’s Radio Operations Center monitor tower sites 24 hours/day, 7 days/week, 365 days/year. Tower sites are gated. All entities that have co-located equipment on MnDOT towers are required to contact the Radio Operations Center when they check in and out.
  - Radio sites have a card key system and a key/deadbolt, for dual access.
  - Equipment shelters have an alarm system on the doors.
- Shelters and DMS have changeable key cores that are changed out after construction.
- Option to add padlocks to equipment cabinets and pole cabinets.
- Communications shelters have key card access and a monitoring system.
- MnDOT uses a Network Management System (NMS) for monitoring long haul communications. Since all field devices are all online, MnDOT staff can clearly see when devices have gone offline, indicating a problem.

## Emerging Practices for Communications Infrastructure

### Interview Summary

Ontario Ministry of Transportation (MTO)

<b>Interview Date and Participant(s)</b>	April 1, 2020 - Phone interview with Paul Lim-Hing, MTO
<b>Current Use of Cellular Services</b>	<p><b>Current Cellular Use for ITS Devices</b></p> <ul style="list-style-type: none"> <li>• Approximately 20% of ITS devices are connected via cellular (LTE), primarily portable dynamic message signs (DMS) along with a few traffic cameras.</li> <li>• MTO uses cellular (LTE) for gateway access (i.e. a hybrid approach), placing modems along the fiber network to connect to devices that aren't on fiber.</li> <li>• Cellular (LTE) modems are deployed at strategic cabinet locations, as a backup in case a fiber outage occurs, to maintain continuity of operations.</li> <li>• Cellular is well-suited for temporary, quick deployments. Some cellular connected camera sites deployed for the 2015 Pan Am Games in Toronto remain operational today.</li> </ul> <p><b>Cost:</b></p> <ul style="list-style-type: none"> <li>• Data rate plans and costs are pre-negotiated with cellular carriers. MTO also negotiated a plan with a vendor to supply modems, which helps to control costs.</li> <li>• After connecting several traffic cameras to cellular, costs escalated due to high usage. Therefore, most cameras with the option to connect to fiber are now back on fiber.</li> </ul>
<b>Use of Emerging Cellular Services</b>	<ul style="list-style-type: none"> <li>• MTO is investigating the use of low-power wide-area network (LPWAN), such as LTE-M offered by cellular carriers in Canada.</li> <li>• LPWAN can be well-suited for communicating to IoT (internet of things) devices that have low bandwidth requirements.</li> <li>• Advantages of LTE-M service: <ul style="list-style-type: none"> <li>– LTE-M offers lower rate plans (e.g. approximately \$15/month for LTE-M compared to \$50/month for LTE). LTE is more expensive to meet higher bandwidth need and provide faster speeds.</li> <li>– Some back-end services are provided with LTE-M, such as the ability to monitor devices, check usage, and manage devices.</li> </ul> </li> <li>• MTO is testing the use of LTE-M for communicating to DMS. It's anticipated that the bandwidth (300kb/sec) capability of LTE-M will be suitable for DMS, but MTO will also test latency, coverage, and overall performance with a test deployment in the field.</li> </ul>
<b>Emerging Trends and CAV Backhaul</b>	<p><b>Edge Computing, Cloud Computing, and "Exception" Communications:</b></p> <ul style="list-style-type: none"> <li>• MTO is moving toward de-centralizing complex data processing functions performing some data processing in the field (i.e. edge computing) or in the Cloud (cloud computing) for certain applications. For example:</li> </ul>

	<ul style="list-style-type: none"> <li>– MTO is deploying Field Traffic Master (FTM) units that complete data processing in the field for ramp metering, travel times on DMS, and other congestion-related messaging on DMS.</li> <li>– Services from 3rd party providers are now available to provide data such as travel times that can be downloaded directly to a field unit to trigger DMS displays, without a need to communicate to a traffic management center (TMC) on an ongoing basis.</li> <li>– MTO is deploying an automated signing strategy for determining messages to post on DMS. This operates using an off-the-shelf application operating in the Cloud, which functions like a virtual TMC. This allows operators to access the application from anywhere. A cellular connection is used to communicate by exception for commands such as over-rides to automated parameters.</li> </ul> <ul style="list-style-type: none"> <li>• While some data processing will continue at a central location, the use of edge and cloud computing will conserve bandwidth and decrease reliance on fiber.</li> </ul> <p><b>Preparing for CAV Backhaul Needs:</b></p> <ul style="list-style-type: none"> <li>• MTO is deploying up to 20 DSRC roadside units (RSUs) along Highway 401, the main corridor through Toronto. The RSUs will be interconnected to 4G LTE modems, for backhaul to TMCs. MTO aims to determine whether 4G LTE is appropriate and sufficient for CAV data backhaul.</li> <li>• Security is a high priority, particularly because there will be many more access points with multiple RSUs deployed for CAV operations. Security strategies include: <ul style="list-style-type: none"> <li>– MTO will acquire LTE modems with built-in firewalls.</li> <li>– MTO will lock down access to ports in switches within field cabinets (e.g. MTO staff or contractors will only be able to plug into a port with an authenticated laptop.)</li> <li>– Rural/remote areas may require additional security measures.</li> </ul> </li> <li>• In the long-term, MTO will continue to investigate infrastructure readiness for CAV operations, considering multiple options including fiber and cellular for backhaul communications. Considerations include security, reliability, capacity, and bandwidth needs: <ul style="list-style-type: none"> <li>– Fiber has been the most secure and reliable option historically.</li> <li>– In terms of capacity, consider whether additional bandwidth use will put too much load on cellular towers in urban areas.</li> <li>– Backhaul choices will depend upon bandwidth required, based on where data processing occurs (e.g. at the cabinet, in the cloud, or at a central location such as a TMC).</li> <li>– Could be a hybrid approach, using both fiber and cellular/LTE.</li> </ul> </li> </ul>
--	---

## Emerging Practices for Communications Infrastructure

### Interview Summary

North Dakota Department of Transportation (NDDOT)

<b>Interview Date and Participant</b>	February 5, 2020 - Phone interview with Russ Buchholz, NDDOT
<b>Current Use of Cellular Services for Long-Distance Communications</b>	<p><b><i>Communication to Field Devices and Current Cellular Use:</i></b></p> <ul style="list-style-type: none"> <li>• North Dakota has a robust fiber network (primarily privately owned and leased by NDDOT) and DOT-owned radio towers, due to good line of sight with flat terrain. The radio towers are connected to fiber for backhaul, and point to point or multi-point is used to connect to field devices.</li> <li>• Cellular communication is used in some locations to connect to ITS field devices throughout the state (e.g. automatic traffic recorders (ATRs), weigh-in-motion (WIM), and some cameras). NDDOT currently uses 3G and 4G cellular service. The DOT operates 190 Verizon field devices and 20 AT&amp;T field devices.</li> <li>• NDDOT construction staff and plow operators use tablets (180+ devices) that push data through Verizon for reporting from the field.</li> <li>• Cellular communication to field device is typically only utilized at locations where other connectivity (e.g. fiber) or power isn't present.</li> </ul> <p><b><i>Cellular Costs:</i></b></p> <ul style="list-style-type: none"> <li>• At this time, cellular services have a monthly fee per device (\$20/month for ATRs, \$38.50/month for WIM and pan-tilt-zoom cameras), with additional charges based on usage. Pan-tilt-zoom cameras and WIM devices have higher charges due to higher usage.</li> <li>• The state has contracts with cellular providers, with pre-negotiated rates. The cellular providers will typically work with NDDOT if there are overages due to weather events or other situations where usage of devices (e.g. cameras) sharply increases from typical usage.</li> </ul>
<b>Emerging Use of Cellular Services for Long-Distance Communications</b>	<p><b><i>Emerging Cellular Services:</i></b></p> <ul style="list-style-type: none"> <li>• 5G buildout is occurring in the urban areas. There's likely not a need for 5G coverage outside the urban environment. 4G and 4GLTE can likely accommodate usage needs in the less populated, rural areas.</li> <li>• <a href="#">FirstNet</a> (nationwide public safety broadband network) is currently primarily deployed in urban areas. FirstNet cellular service is expected to be available in rural areas within two years and is an option for cellular communications to ITS field devices.</li> </ul> <p><b><i>Permitting Small Cell Installations in Agency-Owned Right-of-Way (ROW):</i></b></p> <ul style="list-style-type: none"> <li>• As a standard process, NDDOT turns lighting over to cities after installation, for maintenance and operations. Therefore, the cities will handle most permitting of 5G small cells in the ROW.</li> <li>• A permitting policy is in place for small cell installations in the city of Fargo. NDDOT is developing a policy but doesn't expect many requests.</li> </ul>

	<ul style="list-style-type: none"> <li>• The permitting fee for cellular providers to co-locate on agency-owned ROW is low (\$150/site in the city of Fargo, with a limit of 15 years), therefore carriers are not offering services such as bandwidth in exchange for ROW access.</li> <li>• The city of Fargo policy only allows providers to install new poles for small cell installations due to liability concerns. Installations on agency-owned poles are not allowed. Aesthetic requirements to match in-place conditions/structures must be met by the providers for all new installations.</li> </ul>
<p><b>Selecting Communications to Field Devices</b></p>	<p><b><i>Selection Considerations:</i></b></p> <ul style="list-style-type: none"> <li>• Robust (leased) fiber network and DOT-owned radio towers are the primary means for DOT communications infrastructure to field devices.</li> <li>• NDDOT owns 45 radio towers and has plans to expand to 75 towers statewide. NDDOT is also investing in tower infrastructure by replacing buildings at the current 45 tower locations.</li> <li>• For NDDOT, point to point communication is typically far more economical compared to cellular services, when considering initial investment versus long-term monthly service fees.</li> </ul> <p><b><i>Exception Communications and Developments in Computing Topology:</i></b></p> <ul style="list-style-type: none"> <li>• NDDOT is not trending toward the use of “exception” long-distance communications.</li> <li>• The DOT is considering smart technology (e.g. for wrong way detection, which will need connectivity). NDDOT is also working on an initiative with unmanned aircraft systems (i.e. drones) that utilize radio or cellular communications.</li> </ul> <p><b><i>Preparing for CAV Backhaul</i></b></p> <ul style="list-style-type: none"> <li>• NDDOT has not made any firm decisions for future CAV backhaul communications. Fiber is a viable option. In addition, cellular could be used both for vehicle to infrastructure short-range communications and backhaul with the Federal Communications Commission’s (FCC) proposed rulemaking that would take away the DSRC spectrum for public safety. In rural ND, there is 95% coverage with Verizon and should be able to handle backhaul needs, if cellular is used.</li> </ul>
<p><b>Long-Term Management Practices</b></p>	<p><b><i>Resource Sharing:</i></b></p> <ul style="list-style-type: none"> <li>• NDDOT does not share fiber assets. Nearly all fiber use is leased from a broadband provider. In areas where DOT cameras are located near a city, access to the DOT cameras is provided to the city.</li> <li>• NDDOT does not allow privately own transceivers on DOT-owned towers. However, other government entities (e.g. federal agencies, state radio) are allowed to locate transceivers on DOT-owned towers.</li> </ul> <p><b><i>Tracking Assets:</i></b></p> <ul style="list-style-type: none"> <li>• NDDOT only owns one string of fiber, so tracking is not difficult for this DOT-owned asset.</li> <li>• NDDOT utilizes <a href="#">RadioSoft</a> (AASHTO’s spectrum coordination contractor) for FCC spectrum coordination which is helpful for tracking licenses.</li> <li>• The cities are coordinating on processes to track permits for small cell deployments in the ROW, with the city of Fargo in the lead.</li> </ul>

<p><b>Security</b></p>	<p><b>Physical Security:</b></p> <ul style="list-style-type: none"> <li>• NDDOT has not experienced much vandalism to field devices, with only two vandalism events in the last 10 years.</li> <li>• NDDOT has developed <a href="#">standard specifications</a> for boxes that house components to support field devices. Modifications to the specification have been made to avoid vandalism. For example, increased depth to house more equipment in one box, no longer using a universal key to access it, and the boxes are positioned higher so lift equipment is needed to access the boxes for maintenance.</li> <li>• When other federal or state agencies co-locate transceivers on DOT-owned radio towers, NDDOT provides security and accompanies other agencies' staff to their equipment as needed. An alarm system is present on tower building doors. NDDOT has considered installing a camera on every tower for monitoring and to send alerts with movement detected; however, this has not been implemented.</li> </ul> <p><b>Cybersecurity:</b></p> <ul style="list-style-type: none"> <li>• Cybersecurity is a high priority, both for NDDOT and for the privately owned fiber network. Multiple firewalls are used to secure fiber communications.</li> <li>• Universities are beginning to incorporate cybersecurity training into their curriculum.</li> </ul>
------------------------	---

## Emerging Practices for Communications Infrastructure

### Interview Summary

#### New Hampshire Department of Transportation (NHDOT)

<b>Interview Date and Participants</b>	February 5, 2020 - Phone interview with David Chase and Susan Klasen, NHDOT
<b>Current and Emerging Use of Cellular Services</b>	<p><b><i>Current Cellular Use for ITS Devices</i></b></p> <ul style="list-style-type: none"> <li>• Cellular service is used for selected weather stations, camera trailers, fixed cameras, and dynamic message signs (fixed and mobile).</li> </ul> <p><b><i>Emerging Cellular Use for ITS Devices - FirstNet</i></b></p> <ul style="list-style-type: none"> <li>• Approximately 30 devices are connected to FirstNet.</li> <li>• NHDOT updated their modems at these sites, and FirstNet service has been working well.</li> <li>• NHDOT is an “early adopter” in terms of connecting ITS devices to FirstNet.</li> <li>• A statewide contract with AT&amp;T (FirstNet provider) is in place.</li> <li>• A VPN tunnel between the FirstNet data center and NHDOT network provides a very secure connection for data protection.</li> <li>• FirstNet buildout is occurring in the rural areas of New Hampshire based on the terms of the state’s initial agreement when they opted into FirstNet.</li> </ul>
<b>Selecting Communications to Field Devices</b>	<p><b><i>Selection Considerations:</i></b></p> <ul style="list-style-type: none"> <li>• The primary factors when selecting communications for ITS devices are security, availability, and cost.</li> <li>• Security:             <ul style="list-style-type: none"> <li>– Security is a very high priority when selecting communications.</li> </ul> </li> <li>• Availability:             <ul style="list-style-type: none"> <li>– Availability includes proximity to existing mechanisms (e.g. utilize fiber if nearby).</li> <li>– If using cellular, first choice is FirstNet, as this is the least expensive option, is highly secure, and provides additional user controls and monitoring capabilities with a user portal accessed by DOT staff.</li> <li>– Portable devices (e.g. cameras and message signs) are better suited for cellular, to connect wherever there is cellular coverage.</li> </ul> </li> <li>• Cost:             <ul style="list-style-type: none"> <li>– Costs are highly dependent upon the type of communication used and bandwidth needs.</li> <li>– An upfront cost/benefit analysis is often conducted when selecting communications.</li> <li>– Cellular is becoming more economical and feasible, compared to building infrastructure.</li> <li>– Fiber offers much more bandwidth, but is expensive to build.</li> <li>– Future cost increases (e.g. when leasing tower space or services) are also considered; can’t control escalation rates and future charges are difficult to predict.</li> </ul> </li> </ul>



	<p><b>“Exception” Communications:</b></p> <ul style="list-style-type: none"> <li>Cellular is commonly used for devices that require only “on-demand” communications (not continuously communicating), especially in locations where it’s not feasible to splice into fiber.</li> </ul>
<p><b>Long-Term Management Practices</b></p>	<p><b>Collaborative Broadband Development:</b></p> <ul style="list-style-type: none"> <li>The University System of New Hampshire was the grantee of a broadband opportunity grant which facilitated buildout of a statewide fiber network, in collaboration with state and local governments, non-profits, and private entities. The State of New Hampshire has guaranteed access to the network, with associated cost. See additional information on this initiative “Network New Hampshire Now” at: <a href="https://www2.ntia.doc.gov/grantee/university-system-of-new-hampshire">https://www2.ntia.doc.gov/grantee/university-system-of-new-hampshire</a></li> </ul> <p><b>Tracking Assets:</b></p> <ul style="list-style-type: none"> <li>DOT-owned fiber locations are documented in as-built plans. Other fiber in the state is tracked by the State Department of Information Technology.</li> <li>NHDOT has dedicated staff that obtains, manages, and maintains FCC licenses, utilizing processes such as regular reviews and calendar reminders for required notifications to the commission and renewal opportunity windows.</li> </ul> <p><b>Network Monitoring:</b></p> <ul style="list-style-type: none"> <li>NHDOT uses SolarWinds®, a software platform for monitoring networks, for monitoring network usage and identifying issues.</li> </ul>
<p><b>Security</b></p>	<p><b>Physical Security:</b></p> <ul style="list-style-type: none"> <li>DOT staff make frequent visits to remote sites to check on field equipment.</li> <li>Using alternate locks to traffic cabinets, rather than standard locks that come with the cabinet.</li> <li>An emerging technology of interest is lock technology/key fobs that are adapted for traffic cabinets. While not yet used at NHDOT, this technology can log user activity, control access, and is monitored remotely. Users dock their fobs in order to download usage history and update user privileges.</li> </ul> <p><b>Cybersecurity:</b></p> <ul style="list-style-type: none"> <li>Cybersecurity is a high priority. An example strategy is ensuring that software patches to equipment/devices and communications infrastructure are current.</li> </ul>

## Emerging Practices for Communications Infrastructure

### Interview Summary

#### Utah Department of Transportation (UDOT)

<p><b>Interview Dates and Participants</b></p>	<ul style="list-style-type: none"> <li>• May 12, 2020 - Phone interview with Blaine Leonard, UDOT (selecting communications infrastructure, CAV backhaul, security)</li> <li>• June 3, 2020 – Phone interview with Lynne Yocum, UDOT (fiber sharing, resource exchanges, fiber tracking)</li> <li>• Information gathered via interviews was supplemented with information from online resources, as noted.</li> </ul>
<p><b>Selecting Communications Infrastructure</b></p>	<p><b>Selecting Communications Infrastructure:</b></p> <ul style="list-style-type: none"> <li>• A few ITS devices are connected to cellular, but most are on fiber.</li> <li>• UDOT has access to a robust fiber network. UDOT gains access to fiber for connecting to ITS field devices in two ways:             <ul style="list-style-type: none"> <li>– Installed and owned by UDOT; and</li> <li>– Obtained from private telecommunications providers in exchange for access to UDOT right-of-way or other resource trades.</li> </ul> </li> <li>• Fiber is preferred for communications to ITS devices. Some of the benefits:             <ul style="list-style-type: none"> <li>– Fiber provides a lot of bandwidth and is reliable.</li> <li>– Some rural areas in Utah have very spotty, unreliable cellular service, and some parts of the state have no cellular service at all.</li> <li>– Fiber has no ongoing fees compared to procured services that carry fees.</li> <li>– New technologies enable significant capacity increases to be made to existing fiber, extending the capability of in-place infrastructure to meet data transfer needs for ITS field devices.</li> <li>– Fiber requires less maintenance compared to other types of communications equipment such as cellular modems. Because fiber is underground, it is not impacted by weather.</li> </ul> </li> </ul>
<p><b>Connected Vehicle Backhaul</b></p>	<p><b>Connected Vehicle (CV) Deployments and Data Processing:</b></p> <ul style="list-style-type: none"> <li>• UDOT has CV deployments along two urban corridors with instrumented intersections to enable signal priority for buses and snowplows.</li> <li>• A newer CV deployment, in partnership with Panasonic, is installing roadside units (RSUs), equipping UDOT fleet vehicles with onboard units, building applications to utilize CV data, and building a cloud-based data analytics platform to process CV data.             <ul style="list-style-type: none"> <li>– Data processing will occur in the field for time-critical CV applications including curve warning and weather impact warning.</li> <li>– CV datasets that will be generated at RSUs will be transferred to a central cloud-based application for data processing.</li> <li>– Selected processed information will be communicated to the TMC to support operations.</li> <li>– Other uses (e.g. research) of the CV datasets are being explored.</li> </ul> </li> </ul> <p><b>CAV Backhaul:</b></p>

	<ul style="list-style-type: none"> <li>• UDOT’s existing CV deployments are in urban areas or in outskirts of urban areas. Future deployments will occur in both urban and rural areas.</li> <li>• UDOT’s CV deployments utilize fiber for long-distance communications to and from RSUs in the field. New deployments, even those planned for rural areas, will likely use fiber for data backhaul.</li> <li>• Fiber is the preferred communications mechanism because: <ul style="list-style-type: none"> <li>– Fiber is widely available in many areas within the state; and</li> <li>– UDOT wishes to maintain the ability to transfer large amounts of data from the RSU sites, which fiber can handle.</li> </ul> </li> <li>• Access to fiber is a major consideration when determining RSU deployment locations. Access to power is often more of a concern than access to fiber.</li> <li>• UDOT expects the fiber network to have adequate capacity to transfer CV data and support other ITS field device communications.</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>• Physical security: UDOT is replacing all field cabinet locks with an electronic lock system. Each staff has a key with an RFID chip registered to that person, giving them access to the cabinet for a selected period of time (e.g. 7 days). When this time elapses, staff are required to log in to re-register the key. This system also generates a log of all activity for each key.</li> <li>• Cybersecurity: The UDOT ATMS network (e.g. fiber, field devices) is not directly connected to the internet, securing it from external hacking.</li> <li>• The Security Credentialing Management System (SCMS) will be used to secure the transmission of CV messages for the Panasonic deployment.</li> </ul>
<b>Long-term Management Practices</b>	<p><b><i>Fiber Sharing and Resource Exchanges:</i></b></p> <ul style="list-style-type: none"> <li>• UDOT enters into various sharing and trading arrangements with private telecommunications companies, for example: <ul style="list-style-type: none"> <li>– Telecommunications providers may install fiber on UDOT right-of-way (ROW) in exchange for UDOT use of fiber owned by the provider</li> <li>– Trading use of DOT strands for telecom-owned strands</li> <li>– Small wireless facility installations on UDOT ROW in exchange for use of fiber strands, access to poles, power, or other resources.</li> </ul> </li> <li>• Resource exchanges may or may not be in the location of the negotiated installation. UDOT maintains a balance sheet to track agreements, statuses, and trade values.</li> </ul> <p><b><i>Fiber Tracking:</i></b></p> <ul style="list-style-type: none"> <li>• UDOT tracks its fiber network using the following tools: <ul style="list-style-type: none"> <li>– Bentley is used for the backend database.</li> <li>– Data is converted to Esri (Arc-GIS) for web viewing.</li> <li>– UDOT wrote a script to transfer data from Bentley to ESRI.</li> <li>– An Esri server located at UDOT improves the quality of map viewing.</li> </ul> </li> <li>• UDOT fiber information is available publicly via an online mapping tool: <a href="http://www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9">www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9</a> <ul style="list-style-type: none"> <li>– Information such as conduit size, location, length, owner, planned fiber lines, and splice details can be viewed on the public mapping tool.</li> <li>– The online map is used by UDOT and its partners for planning, locates, and trouble shooting.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>– Credentials are needed to access IP plans and as-builts.</li></ul> <p><b><i>Permitting for Small Wireless Facilities (5G small cells):</i></b></p> <ul style="list-style-type: none"><li>• Processes for permitting and installing small wireless facilities on UDOT ROW can be found at: <a href="https://site.utah.gov/connect/business/permits/small-wireless-facilities-5g/">https://site.utah.gov/connect/business/permits/small-wireless-facilities-5g/</a><ul style="list-style-type: none"><li>– Includes permitting process, fees, installation guidelines, and other resources.</li></ul></li><li>• UDOT maintains an online interactive map for small wireless facilities:<ul style="list-style-type: none"><li>– <a href="https://udot.utah.gov/go/smallwireless5Gmap">https://udot.utah.gov/go/smallwireless5Gmap</a></li><li>– Shows details about each small wireless site, including location, pole details, status, and installation type (new pole or co-location).</li></ul></li><li>• Relocation of Small Wireless Facilities:<ul style="list-style-type: none"><li>– From Utah Code Chapter 21: Small Wireless Facilities Deployment Act <a href="https://le.utah.gov/xcode/Title54/Chapter21/C54-21_2018050820180901.pdf">https://le.utah.gov/xcode/Title54/Chapter21/C54-21_2018050820180901.pdf</a>: 54-21-603 Relocation. (1) Notwithstanding any provision to the contrary, an authority may require a wireless provider to relocate or adjust a small wireless facility in a public right-of-way:<ul style="list-style-type: none"><li>(a) in a timely manner; and</li><li>(b) without cost to the authority owning the public right-of-way.</li></ul></li></ul></li></ul>
--	---

## Emerging Practices for Communications Infrastructure

### Interview Summary

#### Wisconsin Department of Transportation (WisDOT)

<b>Interview Date and Participants</b>	April 1, 2020 - Phone interview with Dean Beekman, Don Schell and Dave Karnes, WisDOT
<b>Current and Emerging Use of Cellular Services</b>	<p><b>Current Use of Cellular Services:</b></p> <ul style="list-style-type: none"> <li>• Approximately 550 field devices utilize cellular including permanent dynamic message signs (DMS), detector stations, portable DMS, and portable cameras.</li> <li>• WisDOT has procured a statewide contract with Verizon: <ul style="list-style-type: none"> <li>– Good reliability and coverage statewide.</li> <li>– Upgraded antennas are used for weak signal areas.</li> <li>– Data rate plans with Verizon for field devices are either a 250 MB plan (\$20/month/modem) or a 1 GB plan (\$25/month/modem) depending on usage. The data can be shared between modems. Available plans go up to 10 GB, however if this much data is needed (e.g. for portable video applications) an unlimited plan is used.</li> </ul> </li> <li>• Other areas within the DOT (e.g. surveying, traffic counts) also utilize cellular service.</li> </ul> <p><b>5G Buildout:</b></p> <ul style="list-style-type: none"> <li>• 5G buildout is occurring in urban areas at locations such as shopping centers where WisDOT has adequate infrastructure and additional bandwidth offered by 5G is not currently needed for WisDOT field devices.</li> <li>• WisDOT will monitor 5G buildout to determine its potential to meet future operational needs.</li> </ul>
<b>Selecting Communications to Field Devices</b>	<p><b>Selection Considerations:</b></p> <ul style="list-style-type: none"> <li>• WisDOT owns an extensive fiber network and has some agreements to lease fiber from third party providers.</li> <li>• The preferred option for field devices is a direct fiber connection. If fiber is not available, cellular is used to connect devices to the fiber network.</li> <li>• Cellular is often used for temporary traffic cameras deployed during road construction projects. When construction is complete, the cameras are often transferred to fiber for ongoing use.</li> <li>• Field devices that utilize third party vendors, such as safety detection/alert systems (e.g. wrong way, over height) and weather stations, are connected via cellular communications.</li> </ul> <p><b>Centralized Computing versus On-Site or Cloud Computing:</b></p> <ul style="list-style-type: none"> <li>• The Wisconsin Department of Administration manages all IT infrastructure for the state agencies at a single data center located in the city of Madison. All servers that support the traffic management center (TMC) reside at this data center and therefore the TMC's complex data computing functions occur at this central location.</li> </ul>

	<ul style="list-style-type: none"> <li>• On-site (edge) computing is used for safety systems that require low latency data processing (e.g. wrong way, over height); these systems are connected with cellular.</li> <li>• Cloud computing applications are being explored but have not been deployed.</li> </ul>
<p><b>Long-Term Management Practices</b></p>	<p><b><i>Wireless Facilities in DOT Right-of-Way:</i></b></p> <ul style="list-style-type: none"> <li>• Wireless facilities such as cellular towers, monopoles, macro cells, small wireless facilities, and their associated equipment may be installed in the right-of-way, as outlined in the WisDOT Highway Maintenance Manual: <ul style="list-style-type: none"> <li>– Highway Maintenance Manual: <a href="https://wisconsin.gov/Documents/doing-bus/real-estate/permits/09-15-41.pdf">https://wisconsin.gov/Documents/doing-bus/real-estate/permits/09-15-41.pdf</a></li> </ul> </li> <li>• A new Wisconsin statute allows cellular providers to install small wireless facilities (i.e. small cells) for 5G in the right-of-way. WisDOT is working with providers to request that they install their own poles rather than co-locating on DOT-owned structures, and to keep electrical systems separate. <ul style="list-style-type: none"> <li>– Wisconsin statutes in Act 14 (small wireless facilities) <a href="https://docs.legis.wisconsin.gov/2019/related/acts/14">https://docs.legis.wisconsin.gov/2019/related/acts/14</a></li> </ul> </li> </ul> <p><b><i>Fiber Assets in Exchange for Right-of-Way Access:</i></b></p> <ul style="list-style-type: none"> <li>• Wisconsin law allows WisDOT to obtain fiber assets from broadband providers in exchange for access to install in the right-of-way. This arrangement has contributed to WisDOT’s robust fiber network.</li> </ul> <p><b><i>Fiber Tracking:</i></b></p> <ul style="list-style-type: none"> <li>• Fiber locations are tracked through as-builts and are documented in spreadsheets and mapping tools such as Google Earth.</li> <li>• WisDOT has tried off-the-shelf tools to track fiber assets, but these were found to be cumbersome and needed dedicated staff to maintain them.</li> <li>• Fiber data monitoring (e.g. monitoring for outages) is performed by a contractor.</li> </ul>
<p><b>Security</b></p>	<p><b><i>Cybersecurity:</i></b></p> <ul style="list-style-type: none"> <li>• WisDOT has worked with Verizon to obtain a Virtual Private Network (VPN) which isolates the agency’s cellular network from the public cellular network. The VPN is typically used for signals and portable devices. Some devices are connected to the public network, in which case the connection is password protected if a connection to an IP address is needed.</li> <li>• Factory default passwords are removed from field devices to mitigate hacking into devices.</li> </ul> <p><b><i>Physical Security:</i></b></p> <ul style="list-style-type: none"> <li>• There is a concern with the use of a common key for all equipment cabinets in the field. In some situations, padlocks have been added to cabinets.</li> <li>• All buildings associated with communication infrastructure have intrusion monitoring systems, and in the future cameras will be added.</li> </ul> <p><b><i>Staffing and Planning:</i></b></p> <ul style="list-style-type: none"> <li>• WisDOT does not have dedicated ITS security staff, however they would benefit from this type of staffing.</li> </ul>

	<ul style="list-style-type: none"><li>• A consultant has been hired to conduct an internal security review of the ITS asset network, to identify risks and vulnerabilities.</li><li>• WisDOT is planning for extra security measures as the City of Milwaukee prepares to host the 2020 Democratic National Convention. Security measures will likely include additional surveillance, additional locks on traffic cabinets, and fencing off selected facilities during the event.</li></ul>
--	--

## Appendix B: Input from Cellular Service Carriers

- AT&T – Interview summary
- Verizon – Company literature provided via email



## Emerging Practices for Communications Infrastructure

### Interview Summary: AT&T

<b>Interview Date and Participants</b>	February 19, 2020 phone interview with Cameron Coursey, Matthew Robertson, Brady Ratchford, and Matt Quinn (AT&T)
<b>Long-Distance Cellular Services</b>	<p><b><i>Current Cellular Services and 5G:</i></b></p> <ul style="list-style-type: none"> <li>• 3G will sunset for some operators leaving 4GLTE and 5G. 5G is being built out. Over time, 5G is expected to deliver latency and capacity enhancements that will enable revolutionary new capabilities for consumers and businesses.</li> <li>• AT&amp;T is developing, testing and deploying 5G use cases with their business customers. Includes The Washington Post, AT&amp;T Stadium and Purdue University.</li> <li>• AT&amp;T is deploying two variants of 5G – “5G+” which delivers ultra-fast speeds over millimeter wave spectrum, and “5G” which will offer nationwide coverage over sub-6 spectrum in the second quarter of 2020.</li> <li>• “5G+”: Delivering ultra-fast speeds and response times, capable of 1+ Gbps, using 5G technology and new spectrum.             <ul style="list-style-type: none"> <li>○ AT&amp;T’s 5G+ service will provide faster speeds than the 5G service, which AT&amp;T began rolling out in late 2019.</li> </ul> </li> <li>• “5G”: 5G over sub-6 GHz spectrum is expected to enable faster responses on new devices.             <ul style="list-style-type: none"> <li>○ Initially expect 5G will offer similar speeds to AT&amp;T’s 5G Evolution technologies.</li> </ul> </li> </ul> <p><b><i>Related links:</i></b></p> <ul style="list-style-type: none"> <li>• Information about AT&amp;T 5G deployments: <a href="https://about.att.com/newsroom/2020/5g_announcements.html">https://about.att.com/newsroom/2020/5g_announcements.html</a></li> <li>• Information about AT&amp;T 5G for business applications: <a href="https://www.business.att.com/portfolios/5G-for-business.html">https://www.business.att.com/portfolios/5G-for-business.html</a></li> <li>• AT&amp;T’s work with The Washington Post: <a href="https://about.att.com/innovationblog/2019/11/att_washington_post.html">https://about.att.com/innovationblog/2019/11/att_washington_post.html</a></li> <li>• Purdue University: <a href="https://about.att.com/story/2019/att_purdue_5g.html">https://about.att.com/story/2019/att_purdue_5g.html</a></li> <li>• AT&amp;T Stadium: <a href="https://about.att.com/story/2019/5g_at_att_stadium.html">https://about.att.com/story/2019/5g_at_att_stadium.html</a></li> </ul> <p><b><i>Transceiver Density and Congestion Control:</i></b></p> <ul style="list-style-type: none"> <li>• Faster speeds can be achieved with multiple channels/transceivers on a tower. For example, if a tower utilizes multiple spectrum carriers, this will increase the speed.</li> <li>• Each tower has resource elements with a “scheduler” that controls and optimizes congestion.</li> </ul>
<b>FirstNet</b>	<ul style="list-style-type: none"> <li>• AT&amp;T has a 25-year contract with the federal government to build out nationwide network to provide first responders with a dedicated priority</li> </ul>

	<p>network (FirstNet) by 2022. More than 99% of the U.S. population already covered by FirstNet today.</p> <ul style="list-style-type: none"> <li>• FirstNet has Primary Users (for use by first responders) and Extended Primary Users (for use by critical public infrastructure owners such as electrical utility companies and transportation agencies). The goal of FirstNet is for Primary Users to have preemption and access to a network at all times, for emergency response operations. <ul style="list-style-type: none"> <li>• FirstNet users use Band 14 (700 MHz) frequency band prioritized to emergency communications), and they can also use the other cellular band.</li> <li>• During an emergency, this band – or lane – can be cleared and locked just for FirstNet subscribers. That means only those on FirstNet will be able to access Band 14 spectrum, further elevating their connected experience and emergency response.</li> <li>• Reaching rural and remote parts of America with AT&amp;T’s FirstNet Band 14 rollout is one of the top priorities. AT&amp;T is enabling their other spectrum assets on cell towers at the same time they are building new ones with the FirstNet band. And in areas where coverage already exists, AT&amp;T is using Band 14 to help first responders get the capacity they need to get the job done.</li> </ul> </li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>• Each use case is scoped and priced individually, based on the customer’s needs, type(s) of applications, and amount of data needed.</li> <li>• Rate plans are often designed based on bandwidth needs, for example low bandwidth (low rate plans) or high bandwidth (higher rate plans) and are not based upon rural or urban environments.</li> <li>• Traffic cameras tend to consume more data, especially in use cases where video is live streamed. These types of use cases would lead to a higher tiered rate plan.</li> <li>• Pooled plans include multiple devices with multiple data “buckets” and flexibility for overages, when the next available data “bucket” can be accessed.</li> <li>• AT&amp;T offers a substantial amount of data plan flexibility with AT&amp;T Control Center: <a href="https://www.business.att.com/products/control-center.html">https://www.business.att.com/products/control-center.html</a></li> <li>• FirstNet pricing: <a href="https://www.firstnet.com/plans.html?tabs=26b46e66-b7ba-4c26-9bf8-63f88b12fb29">https://www.firstnet.com/plans.html?tabs=26b46e66-b7ba-4c26-9bf8-63f88b12fb29</a></li> </ul>
<b>Public-Private Partnerships</b>	<ul style="list-style-type: none"> <li>• Public entities typically procure cellular services through agreements, as opposed to owning cellular towers or paying for cell tower builds.</li> <li>• AT&amp;T is flexible in developing public-private partnerships to exchange goods or services. For example, AT&amp;T has provided “smart city solutions” (e.g. smart lighting elements on poles, digital kiosks, public Wi-Fi access in parks) in exchange for access to agency right-of way, reduced permitting times, or waived permitting fees. Another example is working with an agency to provide a roadside unit as part of a small cell deployment, in exchange for access to the right-of-way.</li> <li>• A few pilot projects conducted by DOTs have deployed roadside units, however it can be difficult for agencies to maintain these units once they are installed. In</li> </ul>

	<p>the future, there could be an opportunity for AT&amp;T to provide a service to manage these roadside units on behalf of the DOT.</p> <ul style="list-style-type: none"> <li>• Here is an example of one of AT&amp;T’s private public partnership initiatives: <a href="https://about.att.com/story/san_jose_public_private_partnership.html">https://about.att.com/story/san_jose_public_private_partnership.html</a></li> </ul>
<p><b>Security</b></p>	<p><b><i>Cybersecurity for Cellular Services:</i></b></p> <ul style="list-style-type: none"> <li>• AT&amp;T offers security services and solutions. A full stack security suite could include cybersecurity consulting Services, managed security services, and a unified security management platform that centralizes threat detection, incident response and compliance.</li> <li>• AT&amp;T provides multiple layers of security including, as a few examples, network security, user managed security, and threat detection/intelligence. Examples include: <ul style="list-style-type: none"> <li>– Network Security: Network security follows globally defined standards and allows for customizable options to add additional layers for AT&amp;T’s Enterprise customers such as private IP address pooling, MPLS connectivity between networks, etc.</li> <li>– User Managed Security: Options exist to create closed user groups (e.g. no one can send an SMS unless they are in the user group, lock down peer to peer, etc.)</li> <li>– Threat detection/intelligence: AT&amp;T Alien Labs Open Threat Exchange, the threat intelligence unit of the company’s cybersecurity organization, delivers analytics-based intelligence for resilient threat identification and response situations, for example if a connection or a device is hacked an immediate action to the break wireless connection can be initiated.</li> </ul> </li> </ul> <p><b><i>Security for Co-Locations:</i></b></p> <ul style="list-style-type: none"> <li>• When AT&amp;T co-locates on infrastructure owned by another party, a site acquisition process takes place. AT&amp;T will design the installation per the owner’s security requirements, and all requirements are determined on a site by site basis.</li> <li>• The infrastructure owners often have gated access or locks, and notification with owner-accompanied access is sometimes required.</li> <li>• For small cell deployments on agency right-of-way (i.e. agency-owned structures or new builds), an agreement needs to be in place to outline how installation and security is handled. This helps to ensure security from the perspective of both parties.</li> </ul>

## Input Provided by Verizon

The following information was provided on July 7, 2021 via email from Keith Hangland, Business Development Manager, Smart Communities - Transportation/Mobility, Verizon.

Verizon is focused on working across a broad spectrum of use cases for 5G Technology and Multi-Access Edge Computing (MEC). Below are several documents to help understand 5G as it relates to roadway automation.

- 1) All kinds of automation and business cases are supported under the 5G framework and the 8 core competencies of the 5G technology outlined in this document. <https://enterprise.verizon.com/resources/casestudies/2019/business-case-for-5g.pdf>
- 2) This whitepaper discusses some of the key benefits and advantages of 5G such as network security, reduced interference of the licensed spectrum, and “network slicing” for highly reliable low-latency connectivity (very important to support automotive use cases): <https://enterprise.verizon.com/resources/whitepapers/2020/5g-vs-wifi.pdf>. This video is helpful to understand 5G as well: <https://www.youtube.com/watch?v=J2xEd8wv4Xs&feature=youtu.be>
- 3) Edge computing is a key component enabling real-time communication and autonomous vehicle technology. Last year Verizon and AWS announced a partnership to bring computing to the edge. This partnership is key to bringing scaling Verizon’s Multi-Access Edge Compute (MEC) technology for automated vehicles and other use cases. See <https://enterprise.verizon.com/business/learn/edge-computing/aws-verizon-edge-cloud-computing-announcement/> For detailed information on MEC please reference <https://enterprise.verizon.com/resources/whitepapers/5g-and-edge-computing.pdf>. Verizon is also working proactively with government and automotive companies as a member of the MCity Leadership Circle industry partners. <https://www.verizon.com/about/news/verizon-5g-ultra-wideband-university-michigan>
- 4) The Verizon Smart Communities program is focused deploying technologies that enable new and cost-effective governments with solutions for fully leveraging the 4G and 5G infrastructure for advanced use cases. These use cases span the transportation, public safety, utilities markets. See <https://enterprise.verizon.com/resources/solutionsbriefs/2020/smart-communities-solutions-brief.pdf>.
- 5) In terms of transportation, the Verizon Smart Communities Mobility team is working with cities and transportation agencies to enhance management of parking, traffic, safety, and automated vehicles. Intelligent roadside video, sensor equipment, and communications technology come together by combining a robust communications framework with AI and machine learning to enable real-time data collection, processing and analytics to power like real-time traffic and infrastructure, Fleet management, and V2X (connected and automated vehicle) technologies.
  - Traffic:

[https://enterprise.verizon.com/resources/solutionsbriefs/2017/reduce\\_congestion\\_with\\_better\\_traffic\\_data.pdf](https://enterprise.verizon.com/resources/solutionsbriefs/2017/reduce_congestion_with_better_traffic_data.pdf)

- Parking:  
[https://enterprise.verizon.com/resources/solutionsbriefs/2020/better\\_insights\\_drive\\_better\\_parking\\_experiences.pdf](https://enterprise.verizon.com/resources/solutionsbriefs/2020/better_insights_drive_better_parking_experiences.pdf)
- Fleet Management:  
[https://enterprise.verizon.com/resources/solutionsbriefs/2018/verizon\\_connect\\_overview\\_solution\\_brief.pdf](https://enterprise.verizon.com/resources/solutionsbriefs/2018/verizon_connect_overview_solution_brief.pdf)
- Automated Vehicle:
  - <https://mcity.umich.edu/verizon-5g-ultra-wideband-network-now-live-at-mcity-test-facility/>
  - <https://www.verizon.com/about/news/verizon-5g-ultra-wideband-university-michigan>
  - <https://www.verizon.com/about/sites/default/files/Mcity-releaseFINAL-CA.pdf>

## References

---

- Arizona Department of Transportation. (July 16, 2020). *State seeks input on leveraging broadband expansion along highways*. Retrieved August 20, 2020 from <https://azdot.gov/adot-news/state-seeks-input-leveraging-broadband-expansion-along-highways>.
- AT&T. (June 15, 2018). *AT&T and City of San Jose Form Smart Cities Public-Private Partnership*. Retrieved August 20, 2020 from [https://about.att.com/story/san\\_jose\\_public\\_private\\_partnership.html](https://about.att.com/story/san_jose_public_private_partnership.html).
- AT&T. (September 5, 2019). *AT&T Reinvents the Live Sports Experience Through 5G at AT&T Stadium with the Dallas Cowboys*. Retrieved August 20, 2020 from [https://about.att.com/story/2019/5g\\_at\\_att\\_stadium.html](https://about.att.com/story/2019/5g_at_att_stadium.html).
- AT&T. (November 21, 2019). *Purdue's College of Engineering Conducting Research with AT&T 5G*. Retrieved March 17, 2020 from [https://about.att.com/story/2019/att\\_purdue\\_5g.html](https://about.att.com/story/2019/att_purdue_5g.html).
- Athey Creek Consultants. (December 2016). *Policies, Laws, and Agreements for the Use of Fiber Communications*. Final Report prepared for ENTERPRISE Pooled Fund Study. [http://enterprise.prog.org/Projects/2015/fiber/ENT\\_Fiber\\_Communications\\_FINAL\\_Report\\_Dec2016.pdf](http://enterprise.prog.org/Projects/2015/fiber/ENT_Fiber_Communications_FINAL_Report_Dec2016.pdf).
- Caltrans. *Wired Broadband Facilities on State Highway Right of Way*. Retrieved August 20, 2020 from <https://dot.ca.gov/programs/design/wired-broadband>.
- Caltrans. *2018 Standard Plans and Standard Specifications*. Retrieved August 20, 2020 from <https://dot.ca.gov/programs/design/ccs-standard-plans-and-standard-specifications>.
- Center for Internet Security. *The 20 CIS Controls & Resources*. Retrieved August 20, 2020 from <https://www.cisecurity.org/controls/cis-controls-list/>.
- Delaware Department of Transportation. (January 2020). *Small Cell in the Right of Way: DeIDOT's Approach*. Presentation P20-21172 for 2020 Transportation Research Board (TRB) Annual Meeting by Eric Cimo, DeIDOT. <https://annualmeeting.mytrb.org/OnlineProgramArchive/Details/14039>.
- Delaware Department of Transportation. *Wireless Small Cell Permits*. Retrieved August 20, 2020 from <https://deldot.gov/Business/WirelessPermits/index.shtml>.
- Eller, A. (Nov 21, 2019). *Guidance for Review of Small Cell Wireless Broadband Deployment on State Assets*. Illinois Department of Transportation internal memorandum. Unpublished.
- ENTERPRISE. *Policies, Laws and Agreements for the Use of Fiber Communications*. Retrieved August 20, 2020 from [http://enterprise.prog.org/Projects/2015/fiber\\_communications.html](http://enterprise.prog.org/Projects/2015/fiber_communications.html).
- Esri. *ArcGIS: The mapping and analytics platform*. Retrieved August 20, 2020 from <https://www.esri.com/en-us/arcgis/about-arcgis/overview>.

Federal Communications Commission (FCC). (September 27, 2018). *FCC Facilitates Wireless Infrastructure Deployment for 5G*. Retrieved August 20, 2020 from <https://www.fcc.gov/document/fcc-facilitates-wireless-infrastructure-deployment-5g>.

First Responder Network Authority (FirstNet). <https://firstnet.gov/>.

FirstNet: About Us. Retrieved March 16, 2020 from <https://firstnet.gov/about>.

FirstNet: Archive. (March 30, 2017). *FirstNet Partners with AT&T to Build Wireless Broadband Network for America's First Responders*. Retrieved March 16, 2020 from <https://2014-2018.firstnet.gov/news/firstnet-partners-att-build-wireless-broadband-network-americas-first-responders>.

FirstNet: Coverage. Retrieved August 20, 2020 from <https://www.firstnet.com/coverage.html>.

FirstNet: History. *FirstNet: The History of our Nation's Public Safety Network*. Retrieved March 16, 2020 from <https://firstnet.gov/about/history>.

FirstNet: Public Safety. *FirstNet for the Extended Community*. Retrieved June 25, 2020 from <https://firstnet.gov/public-safety/firstnet-for/other-users>.

Florida Department of Transportation. *Agencies & New Users*. Retrieved August 20, 2020 from <https://www.fdot.gov/traffic/itsfm/newusersagencies/about-itsfm>.

Florida Department of Transportation. *Lodestar*. Retrieved August 20, 2020 from <https://www.fdot.gov/traffic/its/projects-telecom/lodestar.shtm>.

Illinois Department of Transportation. (November 21, 2019). *Guidance for Review of Small Cell Wireless Broadband Deployment on State Assets*. Memorandum. Unpublished.

Katibeh, M. (November 20, 2019). *AT&T and The Washington Post Team Up to Build the Future of Digital Storytelling*. AT&T Technology Blog. Retrieved August 20, 2020 from [https://about.att.com/innovationblog/2019/11/att\\_washington\\_post.html](https://about.att.com/innovationblog/2019/11/att_washington_post.html).

Krause, C., Anderson, J., Shain, K., Nana, L., Mazzone, T., McNaught, S., and Jackson, M. (September 17, 2019). *Cybersecurity and Intelligent Transportation Systems: Best Practice Guide*. Retrieved August 20, 2020 from <https://rosap.ntl.bts.gov/view/dot/42461>.

Mcity. (September 10, 2019). *Verizon 5G Ultra Wideband network now live at Mcity Test Facility*. Retrieved August 20, 2020 from <https://mcity.umich.edu/verizon-5g-ultra-wideband-network-now-live-at-mcity-test-facility/>.

Minnesota Department of Transportation: Statewide Radio Communications. *Allied Radio Matrix for Emergency Response – ARMER*. Retrieved August 20, 2020 from <http://www.dot.state.mn.us/oec/>.

National Telecommunications and Information Administration (NTIA). *University System of New Hampshire: Network New Hampshire Now*. Retrieved August 20, 2020 from <https://www2.ntia.doc.gov/grantee/university-system-of-new-hampshire>.

NexusWorx. *Fiber Management Made Simple*. Retrieved August 20, 2020 from <http://nexusworx.byers.com/>.

North Dakota Department of Transportation. (October 2014). *Standard Specifications for Road and Bridge Construction*.  
<https://www.dot.nd.gov/divisions/environmental/docs/supspecs/2014StandardSpecifications.pdf>.

Preisen, L., Helgeson, C., and Deeter, D. (October 25, 2019). *Evolving and Phasing Out Legacy ITS Devices and Systems*. Report prepared for ENTERPRISE Pooled Fund Study.  
[http://enterprise.prog.org/Projects/2019/ENT\\_PhasingOutLegacyITS\\_Report\\_FINAL\\_Oct2019.pdf](http://enterprise.prog.org/Projects/2019/ENT_PhasingOutLegacyITS_Report_FINAL_Oct2019.pdf).

Public Law 112-96. (February 22, 2012). *Middle Class Tax Relief and Job Creation Act of 2012*.  
<https://www.congress.gov/112/plaws/publ96/PLAW-112publ96.pdf>.

Ramon, M. and Zajac, D. (January 2018). *Cybersecurity Literature Review and Efforts Report*. Prepared for NCHRP Project 03-127: Cybersecurity of Traffic Management Systems.  
[http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127\\_Cybersecurity\\_Literature\\_Review.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127_Cybersecurity_Literature_Review.pdf).

Raza, U., Kulkarni, P., and Sooriyabandara, M. (2017). *Low Power Wide Area Networks: An Overview*. IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855-873, Second quarter 2017, doi: 10.1109/COMST.2017.2652320. <http://ziyang.eecs.umich.edu/iesr/papers/raza17may.pdf>.

Schafer, A. (August 6, 2019). *Spectrum in 5G: The Innovation Boost Starts Here*. Qualcomm Developer Network. Retrieved March 16, 2020 from <https://developer.qualcomm.com/blog/spectrum-5g-innovation-boost-starts-here>.

SolarWinds. Retrieved August 27, 2020 from <https://www.solarwinds.com/>.

Soracom. *What is LPWAN*. Retrieved June 16, 2020 from <https://www.soracom.io/iot-definitions/what-is-lpwan/>.

Southwest Research Institute. (October 2019). *Cybersecurity of Traffic Management Systems*. Research for NCHRP 03-127. Retrieved August 20, 2020, from <https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179>.

Texas Department of Transportation. (January 11, 2020). *Can you Hear Me Now? TxDOT's Wireless Siting Program*. Presentation P20-21170 for 2020 TRB Annual Meeting by Beverly West, TxDOT.  
<https://annualmeeting.mytrb.org/OnlineProgramArchive/Details/14039>.

Texas Department of Transportation. *Real Property Asset Map*. Retrieved February 6, 2020 from [https://maps.dot.state.tx.us/AGO\\_Template/TxDOT\\_Viewer/](https://maps.dot.state.tx.us/AGO_Template/TxDOT_Viewer/).

Toppen, A., Chambers, J., Ciccarelli, A., Gomez-Martin, L., Daywalt, C., and Berger, K. (September 2019). *Transportation Management Center Information Technology Security*. Final Report prepared for USDOT Federal Highway Administration. FHWA-HOP-19-059.  
<https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf>.

TRB Risk Assessment Web Guidance Tool. Available from <http://cyberguidance.transportationops.org>.



U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA). *Cyber Resilience Review (CRR)*. Retrieved August 20, 2020 from <https://www.us-cert.gov/resources/assessments>.

U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA). (July 23, 2020). *Alert (AA20-205A): NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems*. Retrieved August 20, 2020 from <https://us-cert.cisa.gov/ncas/alerts/aa20-205a>.

U.S. Department of Transportation (USDOT). *Security Credential Management System (SCMS)*. Retrieved August 20, 2020 from <https://www.its.dot.gov/resources/scms.htm>.

Utah Code. (September 1, 2018). *Small Wireless Facilities Deployment Act*. Chapter 21. [https://le.utah.gov/xcode/Title54/Chapter21/C54-21\\_2018050820180901.pdf](https://le.utah.gov/xcode/Title54/Chapter21/C54-21_2018050820180901.pdf).

Utah Department of Transportation. *Small Wireless Facilities (5G)*. Retrieved August 20, 2020 from <https://site.utah.gov/connect/business/permits/small-wireless-facilities-5g/>.

Utah Department of Transportation. *Small Wireless Facilities Installation Guidelines*. [https://www.udot.utah.gov/main\\_old/uconowner.gf?n=3475431509205008](https://www.udot.utah.gov/main_old/uconowner.gf?n=3475431509205008).

Utah Department of Transportation. *UDOT Fiber*. Retrieved August 20, 2020 from <https://www.arcgis.com/apps/webappviewer/index.html?id=096d0a7dd31a4be289b9623935308fc9>.

Utah Department of Transportation. *5G Permitting (Public)*. ArcGIS Web Application of Utah Small Wireless Facilities Interactive Map. Retrieved August 20, 2020, from [www.udot.utah.gov/go/smallwireless5Gmap](http://www.udot.utah.gov/go/smallwireless5Gmap).

Wikipedia. *5G*. Retrieved February 5, 2020 from <https://en.wikipedia.org/wiki/5G>.

Wisconsin Department of Transportation. (March 2020). *Right-of-Way Use & Permits Utility Accommodations: Cellular Installations*. Highway Maintenance Manual Chapter 09, Section 15, Subject 41. <https://wisconsin.dot.gov/Documents/doing-bus/real-estate/permits/09-15-41.pdf>.

Wisconsin State Legislature. (July 10, 2019). *2019 Wisconsin Act 14*. Retrieved August 20, 2020 from <https://docs.legis.wisconsin.gov/2019/related/acts/14>.

Yocum, Lynne. *UDOT Fiber Optic Update 2019*. Presentation slides received from Lynne Yocum, Utah Department of Transportation, via email on June 3, 2020.