



# TRANSPORTATION MANAGEMENT CENTERS

## **Streaming Video Sharing and Distribution**

Final Report



U.S. Department of Transportation  
**Federal Highway Administration**

FHWA-HOP-19-037  
SEPTEMBER 2019

## **NOTICE**

---

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the use of the information contained in this document.

This document is for guidance only and does not create any requirements other than those stipulated in statute or regulation.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear in this report only because they are considered essential to the objective of the document.

## **QUALITY ASSURANCE STATEMENT**

---

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. The FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

**TECHNICAL REPORT DOCUMENTATION PAGE**

<b>1. Report No.</b> FHWA-HOP-19-037		<b>2. Government Accession No.</b>		<b>3. Recipient's Catalog No.</b>	
<b>4. Title and Subtitle</b> Transportation Management Centers Streaming Video Sharing and Distribution				<b>5. Report Date</b> September 2019	
				<b>6. Performing Organization Code</b>	
<b>7. Authors</b> Michael L. Pack, Nikola Ivanov, Elizabeth Birriel				<b>8. Performing Organization Report No.</b>	
<b>9. Performing Organization Name and Address</b> Leidos 11251 Roger Bacon Drive Reston, VA 20190  Michael Pack, LLC, Columbia, Maryland 20145				<b>10. Work Unit No. (TRAIS)</b>	
				<b>11. Contract or Grant No.</b> Contract No. DTFH61-16-D-00053	
<b>12. Sponsoring Agency Name and Address</b> Federal Highway Administration U.S. Department of Transportation 1200 New Jersey Avenue, SE Washington, DC 20590				<b>13. Type of Report and Period Covered</b> Final Report	
				<b>14. Sponsoring Agency Code</b> HOTM	
<b>15. Supplementary Notes</b> Jimmy Chu, FHWA Task Order Contract Officer's Representative					
<b>16. Abstract</b> <p>State and local departments of transportation (DOT) continue to invest heavily in the installation of traffic cameras and distribution of live traffic camera video feeds. State and local DOTs, law enforcement, and transit providers across the country have deployed almost half a million cameras to support transportation and public safety. The video streams from these deployments have the potential to be used for situational awareness, assisting in the response to incidents and events, security and infrastructure monitoring applications, data collection, machine vision, device control, traveler information, and more.</p> <p>The purpose of this document is to synthesize current practices and recommendations for transportation management agencies to share live, streaming traffic camera video with the public, news media, other agencies, and/or trusted partners. This document aims to assist transportation management centers (TMC) in planning, implementing, or improving their sharing.</p>					
<b>17. Key Words</b> CCTV, Video Sharing, Video Distribution, Transportation Management Center.				<b>18. Distribution Statement</b> No restrictions.	
<b>19. Security Classif. (of this report)</b> Unclassified.		<b>20. Security Classif. (of this page)</b> Unclassified		<b>21. No of Pages</b> 100	<b>22. Price</b> N/A



## SI\* (MODERN METRIC) CONVERSION

FACTORS APPROXIMATE CONVERSIONS TO SI UNITS				
SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
<b>LENGTH</b>				
in.	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
<b>AREA</b>				
in. <sup>2</sup>	square inches	645.2	square millimeters	mm <sup>2</sup>
ft <sup>2</sup>	square feet	0.093	square meters	m <sup>2</sup>
yd <sup>2</sup>	square yards	0.836	square meters	m <sup>2</sup>
ac	acres	0.405	hectares	ha
mi <sup>2</sup>	square miles	2.59	square kilometers	km <sup>2</sup>
<b>VOLUME</b>				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft <sup>3</sup>	cubic feet	0.028	cubic meters	m <sup>3</sup>
yd <sup>3</sup>	cubic yards	0.765	cubic meters	m <sup>3</sup>
NOTE: volumes greater than 1,000 L shall be shown in m <sup>3</sup>				
<b>MASS</b>				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
<b>TEMPERATURE (exact degrees)</b>				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
<b>ILLUMINATION</b>				
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m <sup>2</sup>	cd/m <sup>2</sup>
<b>FORCE and PRESSURE or STRESS</b>				
lbf	poundforce	4.45	newtons	N
lbf/in. <sup>2</sup>	poundforce per square inch	6.89	kilopascals	kPa

\*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

## SI\* (MODERN METRIC) CONVERSION (continued)

APPROXIMATE CONVERSIONS TO SI UNITS				
SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
<b>LENGTH</b>				
mm	millimeters	0.039	inches	in.
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
<b>AREA</b>				
mm <sup>2</sup>	square millimeters	0.0016	square inches	in. <sup>2</sup>
m <sup>2</sup>	square meters	10.764	square feet	ft <sup>2</sup>
m <sup>2</sup>	square meters	1.195	square yards	yd <sup>2</sup>
ha	hectares	2.47	acres	ac
km <sup>2</sup>	square kilometers	0.386	square miles	mi <sup>2</sup>
<b>VOLUME</b>				
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m <sup>3</sup>	cubic meters	35.314	cubic feet	ft <sup>3</sup>
m <sup>3</sup>	cubic meters	1.307	cubic yards	yd <sup>3</sup>
<b>MASS</b>				
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
<b>TEMPERATURE (exact degrees)</b>				
°C	Celsius	1.8C+32	Fahrenheit	°F
<b>ILLUMINATION</b>				
lx	lux	0.0929	foot-candles	fc
cd/m <sup>2</sup>	candela/m <sup>2</sup>	0.2919	foot-lamberts	fl
<b>FORCE and PRESSURE or STRESS</b>				
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in <sup>2</sup>

\*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

## TABLE OF CONTENTS

---

<b>EXECUTIVE SUMMARY.....</b>	<b>1</b>
<b>CHAPTER 1. PURPOSE .....</b>	<b>3</b>
<b>CHAPTER 2. BACKGROUND AND LITERATURE SUMMARY .....</b>	<b>5</b>
<b>CHAPTER 3. THE BUSINESS CASE AND DECISIONMAKING PROCESS FOR SHARING OR NOT SHARING .....</b>	<b>11</b>
<b>WHY SOME AGENCIES DON'T SHARE .....</b>	<b>11</b>
<b>WHY MOST AGENCIES SHARE .....</b>	<b>12</b>
<b>AD HOC VS. SYSTEMATIC SHARING .....</b>	<b>15</b>
<b>CHAPTER 4. OPERATIONAL CONSIDERATIONS.....</b>	<b>17</b>
Operator Impacts.....	17
Management Impacts .....	18
Developing a Successful Concept of Operations .....	18
<b>CHAPTER 5. INSTITUTIONAL CONSIDERATIONS.....</b>	<b>21</b>
<b>CONTRACTING.....</b>	<b>21</b>
<b>INTRA-AGENCY COORDINATION .....</b>	<b>22</b>
<b>EQUIPMENT AND NETWORK MAINTENANCE .....</b>	<b>24</b>
<b>CONTINUOUS SUPPORT REQUIREMENTS.....</b>	<b>26</b>
<b>LEGAL IMPLICATIONS .....</b>	<b>27</b>
Memoranda of Understanding and Open Agreements .....	27
Concepts of Operations as a Replacement for an MOU .....	28
Service Charges.....	28
<b>MEDIA .....</b>	<b>29</b>
<b>CHAPTER 6. TECHNICAL CONSIDERATIONS.....</b>	<b>31</b>
<b>NETWORKING .....</b>	<b>31</b>
Network Configuration and Documentation .....	31
Bandwidth Estimation.....	35
Latency.....	35
<b>SECURITY .....</b>	<b>36</b>
<b>VIDEO NORMALIZATION.....</b>	<b>37</b>
<b>KILL-SWITCH TECHNOLOGY .....</b>	<b>39</b>
<b>TECHNOLOGY AND INFRASTRUCTURE MAINTENANCE.....</b>	<b>39</b>

**TABLE OF CONTENTS (CONTINUED)**

---

**CHAPTER 7. HOW TO WORK WITH A SOLUTION PROVIDER..... 41**

**LANGUAGE IN THE REQUEST FOR PROPOSAL.....41**

**CONTRACTOR SELECTION.....42**

**OPERATIONS.....43**

        Before and After Making an Award .....43

**CHAPTER 8. CAMERA AND COMMUNICATIONS EQUIPMENT ..... 45**

    Ideal IP Camera Specifications .....47

    Emerging Features & Technologies .....48

**CHAPTER 9. BUSINESS PRACTICES AND POLICIES..... 51**

**FREE ACCESS.....51**

**RECIPROCAL ACCESS.....51**

**TIERED ACCESS .....52**

**COST RECOVERY MODEL.....53**

**PROFIT MODEL.....53**

**CHAPTER 10. RECOMMENDATIONS ..... 55**

**BUSINESS CASE JUSTIFICATION.....55**

        Operational Considerations.....55

        Technical Considerations .....56

        Concepts of Operations vs. Memoranda of Understanding .....56

        Institutional Considerations .....57

**CHAPTER 11. USE CASES..... 59**

**MARYLAND DEPARTMENT OF TRANSPORTATION .....59**

**NORTH CAROLINA DEPARTMENT OF TRANSPORTATION.....64**

**VIRGINIA DEPARTMENT OF TRANSPORTATION.....66**

        Licensing Issues .....68

**APPENDIX A. EXAMPLE MEMORANDA OF UNDERSTANDING AND  
OTHER AGREEMENTS..... 69**

**APPENDIX B. VIDEO SHARING PRACTICES ..... 79**



## LIST OF FIGURES

---

Figure 1. Map. Transportation agency CCTV deployment map.....	7
Figure 2. Illustration. Common language used to describe transportation system status levels by agencies in the National Capital Region .....	13
Figure 3. Illustration. Information technology and operations interactions .....	23
Figure 4. Diagram. Example of an older many-to-many stream-sharing configuration.....	32
Figure 5. Diagram. Example of many-to-many network configuration.....	33
Figure 6. Diagram. Example of one-to-many stream-sharing configuration.....	34
Figure 7. Illustration. Comparative resolution and aspect ratio chart.....	45
Figure 8. Illustration. Resolution affects the quality of the video and determines what information can or cannot be detected.....	46
Figure 9. Diagram. Original Maryland approach to sharing data and video.....	61
Figure 10. New Maryland architecture: sharing video and data across multiple security zones .....	62
Figure 11. Photo. Example of MDOT’s Service Patrol Mounted CCTV camera.....	63
Figure 12. Photos. Compound figure depicts four examples of on-scene video captured from mobile streaming CCTV cameras mounted in or on service patrol vehicles.....	63
Figure 13. Illustration. North Carolina Department of Transportation media agreement cost language.....	64
Figure 14. Illustration. Unique language from the North Carolina Department of Transportation media agreement requiring that the agency be given 15 public service announcement spots.....	65
Figure 15. Diagram. Virginia Department of Transportation video feed high-level network diagram.....	66
Figure 16. Photo. CCTV feed from the Virginia Department of Transportation 511 system.....	68

## LIST OF TABLES

---

Table 1. Synthesis of transportation agency video sharing as of March 2019.....	8
Table 2. IP Camera resolutions and megapixel equivalent.....	45
Table 3. IP Camera specifications that can enable lower-cost and more feature-rich CCTV streaming to stakeholders .....	47
Table 4. Emerging IP camera technologies beyond traditional transportation management center closed-circuit television camera capabilities .....	48
Table 5. Highlights from three State agency approaches to streaming video .....	59
Table 6. VDOT Media Partner Video Transition Options .....	67

## LIST OF ABBREVIATIONS AND ACRONYMS

---

ATMS	advanced traffic management systems
API	application programming interface
APN	access point name
CCTV	closed circuit television
CDN	content delivery network
CHART	Coordinated Highway Action Response Team
CIF	common intermediate format
CLSP	Clarix live streaming protocol
ConOps	concept of operations
COTS	commercial off the shelf
DASH	dynamic adaptive streaming of http
DDOT	District Department of Transportation (Washington D.C.)
DMZ	demilitarized zone
DOT	department of transportation
EMA	emergency management agency
EMS	emergency management services
EOL	end of life
fps	frames per second
FOIA	Freedom of Information Act
HazMat	hazardous materials
HD	high definition
HEVC	high efficiency video coding
HLS	http live streaming
HTTP	hypertext transfer protocol
IP	internet protocol
ISP	Internet Service Provider
IT	information technology
Kbit/s	kilobits per second
Kbps	kilobits per second
GB	gigabyte
Gbit/s	gigabits per second
Gbps	gigabits per second
MATOC	Metropolitan Area Transportation Operations Coordination
Mb	megabits
MB	megabytes
Mbps	megabits per second

## **LIST OF ABBREVIATIONS AND ACRONYMS (CONTINUED)**

---

MDOT	Maryland Department of Transportation
MITM	man-in-the-middle
MOU	memoranda of understanding
MPEG	Moving Picture Experts Group
MPO	metropolitan planning organization
NCDOT	North Carolina Department of Transportation
NTSC	National Television Systems Committee
PTZ	pan-tilt-zoom
QCIF	quarter common intermediate format
QXGA	quantum extended graphics array
QSXGA	quad super extended graphics array
REST	representational state transfer
RFP	request for proposal
RTMP	Realtime Messaging Protocol
RTSP	Real Time Streaming Protocol
RWIS	road weather information systems
SaaS	Software as a Service
SOP	standard operating procedures
SXGA	super extended graphics array
TCP	Transmission Control Protocol
TMC	transportation management centers
TOC	transportation operations center
TxDOT	Texas Department of Transportation
UPD	unigram data protocol
USDOT	United States Department of Transportation
UXGA	ultra extended graphics array
VDOT	Virginia Department of Transportation
VGA	video graphics array
VPN	virtual private networks
WebRTC	web realtime communication
WVGA	wide video graphics array





## EXECUTIVE SUMMARY

---

State and local departments of transportation (DOT) continue to invest heavily in the installation of traffic cameras and distribution of live traffic camera video feeds. State and local DOTs, law enforcement, and transit providers across the country have deployed almost half a million cameras to support transportation and public safety. The video streams from these deployments have the potential to be used for situational awareness, assisting in the response to incidents and events, security and infrastructure monitoring applications, data collection, machine vision, device control, traveler information, and more.

The purpose of this document is to synthesize current practices and recommendations for transportation management agencies to share live, streaming traffic camera videos with the public, news media, other agencies, and trusted partners. This document aims to assist transportation management center (TMC) staff in planning, implementing, or improving their approach to sharing video feeds.

Some agencies have many and varied reasons to share their video feeds, while others chose not to share their images. Some reasons for not sharing closed-circuit television (CCTV) images include cost concerns and competing priorities. Older cameras, networks and lack of available bandwidth are additional issues that hamper efforts to share images. However, many agencies are resolving these issues and recognize the return on investment they are getting from openly sharing streaming video with both public sector partners and the private sector. The most common benefits of sharing include improved relationships and improved incident management efforts and responses. However, almost all agencies also noted additional benefits, including increasing public good will and trust, meeting public expectations that the desired information is there for general consumption, demonstrating that tax dollars are being used appropriately, and proving to the public that the government is operating openly and transparently.

While a few agencies are trying to recover costs associated with streaming higher quality video to the media and private sector, most agencies are streaming their video feeds at no cost to third parties.

While some agencies have leveraged open-source video sharing software solutions or have built in-house solutions, many agencies are realizing the benefits of outsourcing their video with sharing to third parties or purchasing video streaming appliances that significantly reduce the agency's dependence on in-house, on-call technical staff. This results in the agency's ability to produce enterprise-level, robust solutions that do not inadvertently disrupt the agency's network or core business of traffic management.

Many agencies are also realizing that they can reduce video streaming costs by simply upgrading their aging CCTV cameras to newer IP-based solutions that support multiple streaming profiles.

This document does not discuss older technologies—including static image sharing or motion jpeg technologies. Instead, it focus on true CCTV streaming.





---

## CHAPTER 1. PURPOSE

---

State and local departments of transportation (DOT) continue to invest heavily in the installation of traffic cameras and distribution of live traffic camera video feeds. State and local DOTs, law enforcement, and transit providers across the country have deployed almost half a million cameras to support transportation and public safety. The video streams from these deployments have the potential to be used for situational awareness, assisting in the response to incidents and events, security and infrastructure monitoring applications, data collection, machine vision, device control, traveler information, and more.

There remains a high-demand for access to these video feeds well beyond that of traffic operations. Law enforcement, security, the media, the public, and others routinely request access to State and local DOT cameras. For most agencies, it makes good economic sense to share resources instead of installing multiple cameras. However, each consumer of video has different needs. The media prefers broadcast quality video that can quickly be assessed during traffic reports. Law enforcement desires access to all cameras, usually at the highest resolution and low latency, and they sometimes want control over pan-tilt-zoom functionality. Third party traveler information providers may want access to video to help them produce better reports to be read over the radio, or they may want to redistribute the video feeds on their own websites—driving page views and revenue to their company. The demand for video feeds is so great that many private sector companies have been created that specialize in video redistribution—either as a service to the State and local DOT or as a platform.

Despite the desire, many State and local DOTs often struggle to make their feeds available in the way in which partner agencies and other third parties desire. To make matters worse, there is no uniform guidance for agencies to follow. Agencies and the private sector have not been afforded a platform to openly discuss their approaches, and are not readily sharing lessons learned, business models, processes, contracting strategies, or other solutions. As technologies and markets shift, private sector actors continue to emerge—offering new services, platforms, or other solutions.

Because technologies are changing so quickly, producing a “consumer report” for agencies interested in ranking solutions may not be possible—especially given how much legacy technology (including networks) exists. However, the transportation industry can and should strive to do better—providing guidance for decision makers, legal counsel, network engineers, procurement specialists, systems integrators, and others on how to leverage their existing technologies (at whatever stage they may be). Agencies also need guidance on how to plan for the future when making the business case for sharing video and providing the tools that will enable them to make sharing a reality—regardless of their capability maturity level.

The purpose of this document is to synthesize current practices and recommendations for transportation management agencies to share live, streaming traffic camera video with the public, news media, other agencies, and trusted partners. This document aims to assist transportation management centers (TMC) in planning, implementing, or improving their sharing.

More specifically, this report discusses the different practices that agencies use related to:

- Technologies used.
- Policy considerations.
- Legal issues:
  - Memoranda of understanding (MOUs).
- Funding/costs.
- Operational impacts and other considerations.
- Business practices (fee or free).

The report also synthesizes agencies' experiences, challenges, lessons learned, and recommended practices. The report does NOT cover non-streaming systems (including snapshots or motion jpegs), closed-circuit television video storage, speed enforcement cameras, or red-light running cameras at intersections.

The report further summarize the state of streaming video around the Nation by documenting how many TMCs currently stream their video, to whom, the technologies they use, the differences in approaches and policies, and the reasons why they chose to (or not to) stream. Finally, the report provides guidance on how to work with third parties to enable video stream sharing.

## CHAPTER 2. BACKGROUND AND LITERATURE SUMMARY

Key information for this report came from a mix of in-person interviews, literature reviews, and surveys of public agencies (closed-circuit television (CCTV) deployers), law enforcement officials (CCTV recipients and deployers), other public safety agencies (CCTV recipients), the media (CCTV recipients and deployers), universities (technology providers), CCTV manufacturers, and private sector firms that develop technologies to help owners share CCTV streams. This section summarizes basic facts and figures about sharing around the country, why this is a pressing issue, why it has been difficult for many agencies to share, and why there are so many different approaches to sharing.

While this report focuses on transportation management centers (TMC) and how they share CCTV video, it is important to understand *why* various stakeholders desire CCTV video.



**TMCs:** TMC personnel use CCTV for situational awareness, event detection and confirmation, for coordinating response, for signal timing, for security operations, to monitor critical infrastructure, to understand what equipment to dispatch to a scene, and for public information.



**First Responders (including police, fire, emergency medical services (EMS), safety and service patrols, hazardous materials (HazMat) remediation teams, etc.):** These groups tend to use State department of transportation (DOT) CCTV to gain a better understanding of the status of an incident prior to rolling up on the scene. Knowing what they are responding to can help to reduce surprises and can help to further dispatch the right types of responders, equipment, etc. In addition, first responders may use a State and local DOT's CCTV feeds while on the scene to get a wider view of the area to ensure both their safety as well as that of others on the scene.



**Towing and Recovery:** Towing and recovery personnel make use of live video to understand what equipment might be needed on-scene. Knowing ahead of time how big an incident is can help to ensure the right equipment is dispatched first so that the road can be cleared more quickly. Similarly, towing companies may want to have a better understanding of the space limitations and traffic conditions approaching the scene.



**Media:** For local news stations, the priorities for viewers that drives ratings and advertising revenue are 1) weather, 2) traffic, 3) sports, and 4) news—in that order.<sup>1</sup> Radio follows a similar pattern, with the quality of traffic reporting being extremely high in ratings rankings. Therefore, access to CCTV can dramatically increase viewership, and thus revenue, and is considered a competitive advantage. Several traveler information providers and media outlets interviewed for this project noted that they could attribute the loss or gain of lucrative advertising or other contracts to having access to CCTV from public agencies. These contracts vary

<sup>1</sup> Interview with Regina Hopper, Past President of ITS America and Former Television Reporter.

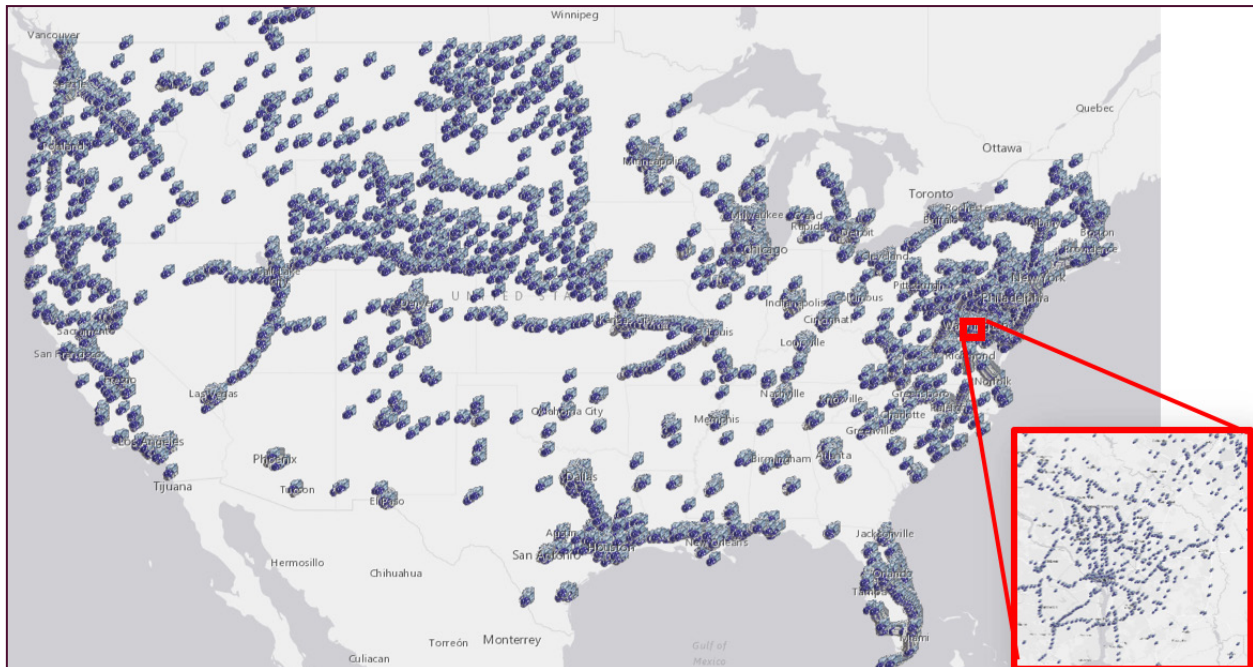
in size and value depending on the markets served and can be as small as \$15,000 per year or can be valued up to millions of dollars. CCTV is particularly valuable because it works for many communication mediums—web, mobile, and broadcast—and it helps the private sector to verify information internally.



**Public:** The public desires access to live CCTV to help make better decisions—especially when an event is detected along their commute route. While navigation apps may alert users of crashes and delays, a video of traffic hazards and conditions can be more compelling. The public also has a general desire to “see” what is happening on the roadway and has become accustomed to live-streaming video from many other outlets.

Despite the desire from multiple stakeholders, there is a great disparity among transportation agencies when it comes to their willingness and ability to share their own video feeds with third parties. Some agencies have fully solved their video distribution issues; however, due to local conditions, their solution may be impossible for another agency to replicate. Some common barriers include: network capacity, analog to digital conversion, compression, an unhealthy mix of multi-generational technologies, and more.

Other public agencies (including both State and local DOTs, law enforcement, emergency management agencies, MPOs, etc.) may have a technical solution ready, but they have yet to resolve political, financial, operational, or other institutional challenges. For example, the leadership within the agency may be sensitive to privacy and security concerns. A culture of fear can paralyze an agency’s progress towards collaboration—even with partner agencies. Sometimes, an agency’s IT policies prevent it from implementing the correct solution, or any solution at all. In these instances, lack of understanding and collaboration between agency IT and operations departments results in loss of significant capability for the agency. In other instances, the agency may not have the right information to justify the expense of implementing a sharing solution. In a few cases, agencies are even “held hostage” by third parties that manage (or outright own) the agency’s CCTV platforms and are either unwilling to allow sharing, artificially inflate costs to discourage sharing, or have entered into exclusive relationships with select media partners that inhibit further distribution. There is even one situation in which an agency developed their video sharing memoranda of understanding (MOU) in a vacuum, with the end result being an MOU that was so restrictive that no other partner agency could convince legal counsel to accept the terms and conditions of the agreement.



**Figure 1. Map. Transportation agency CCTV deployment map.**  
 Source: FHWA. “Federal Highway ITS Asset Viewer – Geospatial Viewer for ITS Assets” web page.  
 Available at: <https://www.itsassets.its.dot.gov/>, last referenced May 1, 2019.

The 2016-2017 Deployment Tracking Survey<sup>2</sup> by the U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office found that 44 of the 50 responding agencies were sharing realtime video data in some form. The survey did not specify whether this referred to video streams or static snapshots. Agencies focusing on arterial management were less likely to be sharing their CCTV realtime video (25 percent of all responding agencies). Roughly 7 percent of transit agencies that responded to the same survey claimed they were sharing their realtime video data.

While the above survey is less than 3 years old, technology—the public’s desire for streaming video feeds—is changing rapidly. Table 1 provides the results of an informal March 2019 survey of the top 50 TMCs in the Nation and other TMCs with respect to their CCTV assets and ability to share/stream live video.

2 U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office. (n.d.). “2016-2017 Deployment Tracking Survey Results.” Available at: [https://www.itsdeployment.its.dot.gov/fm\\_ic.asp](https://www.itsdeployment.its.dot.gov/fm_ic.asp). Last accessed May 1, 2019.

**Table 1. Synthesis of transportation agency video sharing as of March 2019.**

Agency or TMC	Number of CCTV Cameras	Shared with other Agencies?	Shared with the Media	Shared Directly with the Public	Cost recovery for sharing?	Plans to share in the near future?
Alabama DOT	~500	✓	✓	✓	NO	N/A
Arizona DOT	450	✓	✓	✓	NO	-
Arkansas DOT	80	✓		✓	NO	N/A
California DOT	2889	✓	✓	✓	NO	N/A
Colorado DOT	600	✓	✓	✓	NO	N/A
Connecticut DOT	342	✓	✓	✓	NO	N/A
Delaware DOT	252	✓	✓	✓	NO	N/A
District of Columbia DOT	220	✓	✓	✓	NO	N/A
Florida DOT	3292	✓	✓	✓	YES	N/A
Georgia DOT	1250	✓	✓	✓	NO	N/A
Idaho DOT	244	✓	✓	✓	NO	N/A
Illinois DOT	250	-	-	✓ (only 1)	NO	-
Indiana DOT	350	✓	✓	✓	NO	N/A
Iowa DOT	400+	✓	✓	✓	NO	N/A
Kansas DOT	120					
Kentucky DOT	224 snapshots	-	-	✓	NO	N/A
Louisiana DOT	~500	✓	✓	✓	NO	N/A
Maryland DOT	950	✓	✓	✓	NO	N/A
Massachusetts DOT	-	✓	-	-	-	YES
Michigan DOT	760	✓	✓	✓	NO	N/A
Minnesota DOT	1000	✓	✓	✓	NO	N/A
Mississippi DOT	977	✓	✓	✓	NO	N/A
Missouri DOT	1154	✓	✓	✓	NO	N/A
Nebraska DOT	234	✓	✓	✓	NO	N/A
Nevada RCTO	700	✓	✓	✓	NO	N/A
New Jersey DOT	1080	✓	✓	✓	NO	N/A
New York State DOT	1015	✓	✓	✓	NO	N/A

**Table 1. Synthesis of transportation agency video sharing as of March 2019 (continued).**

Agency or TMC	Number of CCTV Cameras	Shared with other Agencies?	Shared with the Media	Shared Directly with the Public	Cost recovery for sharing?	Plans to share in the near future?
New York City DOT	600	✓	✓	✓	NO	N/A
North Carolina DOT	-	-	✓	-	NO	YES
North Dakota DOT	118 snapshots	-	✓	✓	NO	-
Ohio DOT	700	✓	✓	✓	NO	N/A
Oklahoma DOT	268	✓		✓	FUTURE	
Oregon DOT	425	✓	✓	✓	NO	N/A
Pennsylvania DOT	950	-	-	-	-	
Rhode Island DOT	143	✓	✓	✓	NO	N/A
South Carolina DOT	500	✓	✓	✓	NO	N/A
Tennessee DOT	551	✓	✓	✓	YES	-
Texas DOT	652	✓	✓	✓	NO	N/A
Utah DOT	1400		✓		NO	
Vermont DOT	45 snapshots				NO	N/A
Virginia DOT	-	✓	✓	✓		N/A
Washington DOT	1200	✓	✓	-	NO	-
West Virginia DOT	113	✓	✓	✓	NO	N/A
Wisconsin DOT	30	-	✓	-	NO	-
Wyoming DOT	171 snapshots	-	-	✓	NO	-

- = no data. CCTV = closed circuit television. DOT = department of transportation. TMC = transportation management center.





## CHAPTER 3. THE BUSINESS CASE AND DECISIONMAKING PROCESS FOR SHARING OR NOT SHARING

---

### WHY SOME AGENCIES DON'T SHARE

The primary reasons why some agencies are not sharing their streaming closed-circuit television (CCTV) include the following:

**Cost Concerns:** Agencies that are not currently sharing have stated that the expected cost of sharing CCTV has been their largest hurdle. CCTV sharing was not seen as a necessary activity, and agencies expressed concerns that this could divert funds away from other priorities. Agencies that were concerned about cost, however, rarely knew how much other agencies were paying for their streaming solutions and had not costed out their own solutions. Therefore, it is not clear if this is an actual issue or if it is simply a perception.

**Lack of Technical Capacity:** Many agencies, such as State and local departments of transportation (DOTs) and law enforcement, lack the technical expertise to develop or implement streaming video solutions on their own. Streaming video requires a mix of expertise and knowledge of agency networks, firewalls, communication protocols, streaming equipment, camera technologies, and more. Even writing an effective request for proposal to bring in a consultant can seem like a daunting task for some agencies.

**Dated Cameras and/or Networks:** As will be described later, the types of camera technologies deployed and the agency's own communications networks can have a financial impact on streaming solutions. Agencies with older or outdated camera technologies, limited bandwidth, etc. seem less likely to be sharing their videos with the public, third parties, etc. If they are sharing, they are the ones more likely to be charging for access to their video streams.

**Competing Priorities:** State and local DOTs are facing many challenges associated with shrinking budgets and smaller staff. As resources become scarcer, CCTV sharing can be easily thrown to the bottom of an individual's (or agency's) to-do list.

**Lack of Reciprocity:** At least one agency noted that while they were willing to share with agency partners, these potential partners were not as enthusiastic about sharing with them. Reciprocal sharing was a key motivator for this particular agency, and the unwillingness of the partner to share was a setback. While this did not outright kill the agency's sharing initiative, it took well over a year to resolve and realize the benefits of sharing.

**Political and Legal Roadblocks:** Other agencies have stated that they are struggling with internal roadblocks, including:

- Lack of management support.
- Legal concerns or overly complicated memoranda of understanding (MOUs) that tend to deter rather than facilitating third-party access.

- Fear of retribution if the system isn't up 100 percent of the time, and legal concerns if the streams become unavailable when they are needed the most during the management of a critical incident.
- Fear that some (or all) of the agency's CCTV streams could be used against them or be a security risk if terrorists or criminals were to gain access.
- Fear of losing control of the agency's CCTV assets if another agency with a higher political standing were to realize what the State and local DOT's capabilities were.
- Fear over the sharing of personally identifiable/sensitive information when operators need to zoom in to crash scenes.

## WHY MOST AGENCIES SHARE

As documented in chapter 2 of this report, many agencies are either already sharing their CCTV streams or desire to do so in the near future. Each agency has made its own business case for doing so, but the most common business justifications include:

**Incident Response:** Police, fire, hazardous material remediation, other emergency services, and even towing and recovery are all part of a team of professionals working together to respond to incidents. A key goal of the State and local DOT is to safely and quickly clear incidents from the roadway. The majority of State and local DOTs sharing video today noted that it was important to provide responders with critical information about the nature of the incident before they arrived on the scene. Sharing video with other first responders (including towing and recovery) aided in the response effort as they had a better understanding of what they were going to be dealing with before rolling up on scene.

**Reciprocal Sharing:** Several State and local DOTs noted that they had a strong desire to gain access to cameras owned by other agencies (police or local DOTs), and they were able to get access to these additional video feeds only after they offered up their own CCTV assets to those reciprocal agencies. The act of sharing encouraged others to share, which increased the State and local DOT's overall situational awareness and coverage area.






**Improved Relationships:** Many State and local DOTs noted that the very act of sharing their video streams with other agencies has dramatically improved interagency coordination. By providing video, other agencies have become more receptive to sharing other pieces of information, which has led to greater overall coordination and cooperation.

**Winter Weather Coordination:** Several State and local DOTs noted that they leverage CCTV sharing technologies to help communicate amongst one another during winter weather operations. Maryland, the District of Columbia, and Virginia, for example, use CCTV video to assess each other's road networks and to ensure each agency is using the same language to communicate with one another and with the media. Figure 2 was developed by the Metropolitan Area Transportation Operations Coordination (MATOC) member agencies. Each State and local DOT and public safety agency in the region uses this chart along with live CCTV streams to determine how to communicate with the public and one another when describing their road conditions before, during, and after winter weather events. Without access to each other's video streams, the agencies would not be able to communicate as effectively with each other and the media.



Updated: 09/17/12

**MATOC Severe Weather Coordination Working Group  
Transportation System Status Levels**

TABLE 1: Transportation system status levels		Suggested terminology and PIO templates
<p><b>Road Condition 5: IMPASSABLE/ DANGEROUS/ TREACHEROUS</b></p> <p>Some roads could be temporarily impassable. This may be the result of severe weather (low visibility, etc.) or road conditions (drifting, excessive unplowed snow, glare, ice, accidents, stranded vehicles, etc.) Skeletal transit services. Limited above-ground rail service if more than 8" of accumulation. Lane drops in certain sections.</p>		<p>"treacherous", "impassable", "dangerous" <i>Be where you need to be by &lt;time&gt;.</i>  <i>Get where you need to be before the weather gets bad.</i>  <i>Stay where you are.</i></p>
<p><b>Road Condition 4: ICY/SNOW PACKED</b></p> <p>The pavement surface is covered with packed snow and/or ice. There may be loose snow on top of the icy or packed snow surface. Transit lifeline services only with significant delays for rail and bus. Refreeze possible. Lane drops in certain sections.</p>		<p>"unsafe", "impassable" "major delays" <i>Be where you need to be by &lt;time&gt;. Avoid or postpone travel for next &lt;hours&gt;.</i>  <i>Stay at the office an extra &lt;hour&gt;, or leave early, to avoid travel during a winter storm.</i></p>
<p><b>Road Condition 3: SNOW AND/OR SLUSH COVERED</b></p> <p>The pavement surface has continuous stretches of packed snow with or without loose snow on top of the packed snow or ice. Core bus services only, delays in rail services. Lane drops on certain sections of roadways.</p>		<p>"caution", "passable"  <i>Avoid being stranded at bus stops</i>  <i>Avoid or postpone travel for next &lt;hours&gt;.</i>  <i>Stay off the roads.</i>  <i>Stay at the office an extra &lt;hour&gt;, or leave early, to avoid travel during a winter storm.</i></p>
<p><b>Road Condition 2: SNOW / SLUSH COVERED W/ WHEEL TRACKS EXPOSED</b></p> <p>Accumulations of loose snow or slush up to 2 inches are found on the pavement surface. Packed and bonded snow and ice are not present. Regular transit services with some minor exceptions and detours for buses. Drifting snow.</p>		<p>"passable"  <i>Avoid discretionary travel. Road crews engaged in clearing activities.</i>  <i>Curtail "elective" travel. Avoid unnecessary travel.</i></p>
<p><b>Road Condition 1: CLEAR WET/DRY</b></p> <p>Clear and wet/dry pavement surface is the general condition. There are occasional areas having snow or ice accumulations resulting in drifting, sheltering, cold spots, frozen melt-water, etc. Transit operations per schedules.</p>		<p>"passable"</p>

© 2012 Maryland Center for Advanced Transportation Technology

**Figure 2. Illustration. Common language used to describe transportation system status levels by agencies in the National Capital Region.**

Source: University of Maryland Center for Advanced Transportation Technology, MATOC Program.

**Traveler Information:** A better informed public can make better decisions. If you can get people to make better travel decisions (like avoiding certain roads, changing departure times, etc.) then you can reduce congestion and reduce secondary incidents. Good traveler information can save lives, and providing video of incidents to the public (either directly or through the media) is a key component of that—especially given how impactful video can be on public perception. A video showing a four-car pileup and incredible traffic queues is far more impactful than a map showing a simple incident icon and a red-colored road.

**Good Will/Public Trust:** State and local DOTs are frequently looking for ways to show the public and legislators the value of operations and traffic management. Free and open access to streaming video from transportation management centers has been seen by some State and local DOTs as an important part of communicating the value of transportation management centers (TMC) and in gaining public trust in the important work that is being done to make roads safe and efficient.

**Public Assets:** Many State and local DOTs felt that taxpayers had already funded the purchase and deployment of the CCTV cameras, and that there was a sense of duty to provide live video back to the public as a way to show additional return on investment.

**Public Expectation:** The public can now easily stream live video from just about any mobile device to their own web pages, to YouTube Live, through Facebook, FaceTime, Google Hangouts, screen-sharing apps, etc. With the explosion of live video sharing/streaming technologies and solutions available to the public, there is a general expectation from the younger generation that streaming video is the norm rather than the exception. With this growing expectation, many State and local DOTs simply feel pressure to share because “everybody else is doing it.” There is a sense of embarrassment among some State and local DOTs that were not previously sharing their video streams.

**Supporting Business:** Several State and local DOTs noted that the sharing of CCTV streams played a small role in economic development and job creation, and that, overall, providing CCTV streams supported businesses. This is due to the fact that many traveler-information businesses (including television and radio media companies) derive revenue from advertisers and others through traffic reporting and access to CCTV streams. While it may seem small, free and open access to CCTV streams helps with local economies, job creation, etc. Most State and local DOT personnel interviewed shared a common view of CCTV streaming, and provided quotes similar to the quotes below:

“As we worked towards the sharing of our (and other) video streams, we found it important to worry less about what we are going to get out of the sharing of video streams, and instead focus on how video (and other information) sharing will benefit everyone—first responders, the public, etc. We are all part of the same team—trying to make the roads safer and more efficient.”

~*Maryland Official*

“Our video streaming solution gives TDOT [Tennessee Department of Transportation] so much more flexibility in managing and sharing realtime video with partner agencies and the public. Having realtime video available on virtually any device is a significant enhancement for TDOT's video infrastructure and highway event management capabilities.”

~*Michael Nichols, Sr. Project Manager | Tennessee Department of Transportation*

“Our video sharing solution has already had a large positive impact on the situational awareness of our Traffic Management Unit. Management and users alike are very pleased with the product.”

~*Scott Hoffman, Manager of Network Operations | Pennsylvania Department of Transportation*

## AD HOC VS. SYSTEMATIC SHARING

For agencies that do share their video streams, each had to make a business decision about how to share its video. While the specifics of these decisions are discussed in latter chapters, they generally fall into two categories of sharing: ad-hoc vs. systematic.

Ad-hoc sharing means that the agency does not have a direct plan for sharing its video data or a specific system developed to allow for scalable video distribution. Instead, the agency waits for a third party to request video, and then they work with that party to determine how to share that video. The way in which such agencies share their video may vary greatly from one party to another. With this style of video sharing, agencies may frequently encounter redundant sets of hardware, network connections, etc. within a State and local DOT's operations center—each potentially taking up a lot of space and drawing a lot of power.

Systematic sharing, however, is very different. Agencies that share their video systematically have set up rules or a dedicated technical solution for sharing video streams. When any third party comes to the State and local DOT asking for access to video, the State and local DOT is ready with an existing solution for sharing—thus standardizing technologies, networking requirements, etc.



---

## CHAPTER 4. OPERATIONAL CONSIDERATIONS

---

Closed-circuit television (CCTV) sharing is often viewed as a technical problem to be solved; however, CCTV sharing can impact operations, the operator, and other policies directly in the transportation management center (TMC). As mentioned in the prior chapter, the vast majority of agencies see positive operational impacts resulting from CCTV sharing; however, the following factors should be considered.

### Operator Impacts

**Public Cutoff Switch:** Some agencies have decided that they will have two separate video feeds for each and every camera. Feeds for trusted partners (like first responders) are continuously streamed regardless of how far zoomed in the camera may be, what is being shown, etc. Feeds for the media and the public website may be outfitted with cutoff or kill switches that are enabled when the agency needs to zoom in close to an event that may contain sensitive information, particularly gruesome images, etc. These cutoff switches are optimal from a technology standpoint, but do require a change to standard operating procedures (SOPs) within the operations center. The implications to operators and operations may change depending on the partner type:

- **Trusted partners** (EMAs, First Responders, etc.)—These partners would experience little negative impact as cutoff switches are not necessary. Conversely, a significant positive impact can be expected resulting from coordinated response and relationship building, as discussed in chapter 2.
- **The media**—These organizations would experience some impact depending on the technical setup. If an agency has a cutoff switch for when an operator must zoom in to particularly gruesome incidents, then the operator must be mindful of when to turn on/off the switch. Prolonged video cutoff can lead to an increase in calls from the media and the public wondering why the video is turned off, which can potentially overload the operators. If the agency does not have a kill switch, then it may be necessary to have an agreement (or understanding) with the media that governs when they should or should not broadcast certain types of video. Having these types of conversations with the media can have positive impacts on the relationship between the State and local DOT and the media, and can yield better coordination and collaboration in the future.

**Pan-Tilt-Zoom (PTZ) Control:** The vast majority of agencies only stream their video feeds and do not provide actual PTZ control to other agencies. However, if PTZ is granted to third parties, the agency TMC staff will need to enact SOPs that dictate when third parties can have control, and how to resolve conflicts when one agency wants to pan left and another wants to pan right.

**Zooming and Privacy:** If the agency does not have a cutoff switch and is sharing its video freely and openly with the public, the agency may decide to restrict operators from zooming in to incident scenes too closely to avoid triggering privacy concerns.

**Dashcams:** Several agencies now have dashcams and/or PTZ cameras mounted to the top of their service patrol and maintenance vehicles. These cameras offer TMC personnel additional insights into conditions on the ground and provide coverage where pole-mounted cameras are not located.

Some agencies have had to change standard operating procedures (SOPs) for both their field and center personnel to account for these new cameras. Field personnel must be instructed when to turn on or off the camera (if they are not automatically turned on when the vehicle is operational). Among TMC personnel, some agencies have created additional protocols that dictate radio communications to the vehicle operator before video streams can be viewed (in case the operator may be on a break, at home, etc.) to address privacy concerns. At least one agency, however, has recently changed their SOPs to automate many of these protocols and has otherwise relaxed rules that would have increased operator workload.

## Management Impacts

**Uptime Expectations:** Once an agency decides to share video, some managers begin to worry about expectations from partner agencies, the media, and the public on the availability of their video streams. If an agency is managing the system internally, there can be an increased workload and strain on employees to maintain an acceptable level of service that does not embarrass the agency or needlessly divert staff away from other critical tasks.

**Cost:** While there are significant operational benefits to sharing CCTV with others, doing so is not free. Managers must weigh the cost of providing these video feeds with the cost of not sharing the feeds. With constrained fiscal environments, managers must also determine if sharing CCTV feeds is more important than other competing programs. This has caused a level of stress for some managers, leading some to evaluate if they should monetize their CCTV feeds to recoup their own costs of providing video to others. In such cases, managers are then obligated to evaluate the cost and burden of attempting to monetize the feeds to determine if they can develop, implement, and manage a fair and sustainable cost-recovery program. Said one State DOT manager interviewed for this document, “the juice is rarely worth the squeeze.”

The majority of agencies interviewed for this report noted that CCTV video is only truly valuable and beneficial when it is openly shared with all “need to know” agencies, and that any roadblock to sharing is generally viewed as both detrimental to the health, safety, and efficiency of the transportation system as well as counterproductive to achieving the significant benefits documented in chapter 3.

## Developing a Successful Concept of Operations

Agencies that spend time developing philosophical principles of video sharing have been more successful in developing stable, well-funded, and impactful video sharing relationships that are more resilient when agencies or their partners experience changes in leadership. Examples of other agency concepts of operations (ConOps) are provided in appendix A, but some overarching themes to the more successful systems in operation today include:

1. Signed MOUs that have restrictive language, imposing legal references, or require that participants abide by the laws of a specific State are avoided at all costs. Some of the larger sharing systems do not have any MOUs at all, but rather stick to a guiding set of principles in a simple ConOps document.



2. All CCTV video remains the exclusive property of the originating agency and may be used only with permission by the originating agency. Example language: “All live video remains under control of the Originating Agency, both for sharing with other agencies, the public, or in response to disclosure requests under public information laws or discovery requests.”
3. The originating agency will maintain PTZ control of their video system’s cameras. The originating agency has full discretion to approve or deny requests for PTZ changes or control by any other participating partner agency on a case-by-case basis.



## CHAPTER 5. INSTITUTIONAL CONSIDERATIONS

---

Agencies that are sharing closed-circuit television (CCTV) streams (or looking for ways to establish sharing mechanisms) must consider institutional challenges associated with this activity. Some of the institutional challenges will be similar to other existing agency activities, including incident data sharing, resource sharing with partners, public relations, etc. Other challenges are unique to CCTV stream sharing because of the nature of CCTV streams. For example, streams expose images or activities that may not be suitable for the public (e.g., incident scenes, police activity, etc.), so tight control of what is shown, when, and to whom is more critical than in other cases. Public perception of surveillance makes implementing sharing techniques more sensitive than sharing generic travel data, which may appear to be less invasive to the public. Further, CCTV streaming involves constant transmission of large amount of data, which requires specific network and hardware considerations.

Institutional considerations relative to CCTV stream sharing include the following overarching categories:

- Contracting.
- Intra-Agency Coordination.
- Equipment and Network Maintenance.
- 24/7 Support Requirements.
- Legal Implications.
- Public Perception.
- Media and Political Pressure.

### CONTRACTING

Contracting can come into play during multiple phases of CCTV sharing. Agencies may wish to contract for equipment, services, or staff support to help in developing and implementing CCTV streaming solutions. Each agency will have its own contracting challenges mainly associated with procurement. For example, some agencies have expertise with contracting for services but not for hardware. Other agencies have the opposite problem.

When negotiating contracts with the private sector, agencies should be open, honest, and have frequent discussions with potential bidders. Good communication will lead to fewer surprises and less disappointment for both the agency and the contractor.

Once an agency is able to share streaming video, it may develop additional contracts with third parties looking to purchase or otherwise fund access to those CCTV streams. This attempt to monetize (or recover costs associated with) streaming video frequently runs into contracting issues. States and local governments are not typically set up to receive funding or be seen as potentially making a profit. Agencies like the Tennessee Department of Transportation have spent time and energy developing contracting methods to receive funds from the private sector.

Other agencies have determined that the work involved to recover relatively small sums of money simply is not worth the effort.

If an agency does decide to develop a contract that allows for cost recovery or revenue generation, the agency will need to consider the following:

- IT/networking costs (the primary reason for cost recovery with CCTV streaming).
- 24/7 operations and maintenance support.
- 24/7 technical/user support.
- Contracting/management/legal (which can be more than networking costs if only a small number of subscribers are expected).
- Periodic system upgrades.
- Insurance/liability—though some States are self-insured.

It is important to think about contracting costs and legal fees. Even if agency staff do not officially charge their time to specific projects, there is a real cost to these additional contracting efforts. Agencies must also think about how dealing with third-party CCTV contracting may pull limited agency resources away from other, potentially more important projects.

## **INTRA-AGENCY COORDINATION**

Most agencies have stand-alone information technology (IT) departments that manage multitude of IT-related activities ranging from transportation management center (TMC) workstation maintenance to network and security management to ITS equipment interfaces management to software installation and procurement. As transportation operations continue to rely on technology, the overlap between IT and operations increases. Some agencies have addressed this shift by identifying opportunities to collaborate across IT and operations to maximize their investment and resources. Unfortunately, this is more of an outlier than the norm. Many agencies still struggle with internal “silos” where IT and operations exist as separate entities with their own missions, goals, and budgets, and the coordination and cooperation with operations is limited or non-existent. This often results in conflicting approaches to solving problems, unnecessary waste of resources, and “power-struggles” when it comes to decisions and control of resources and equipment.

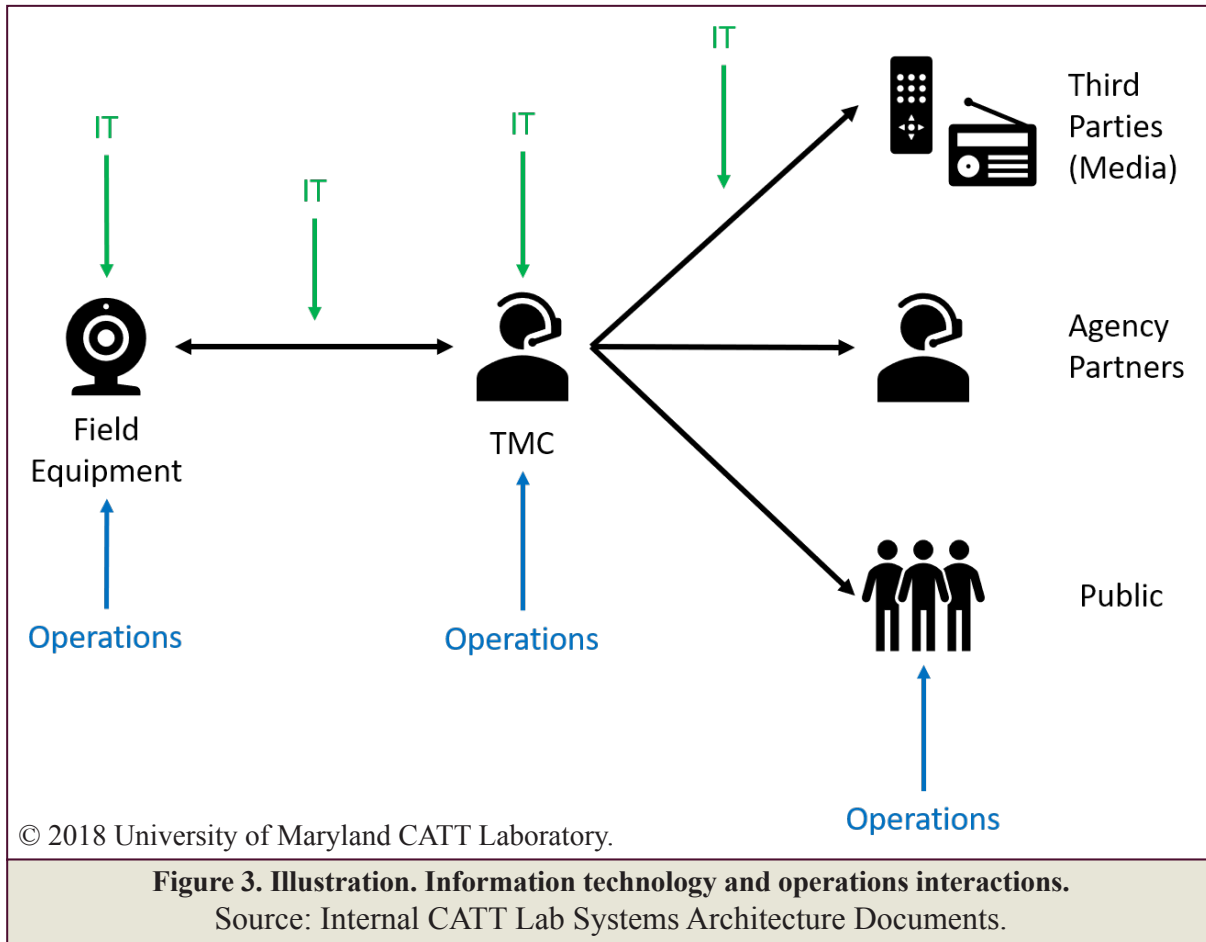
CCTV stream sharing is an activity that can be significantly impacted by these intra-agency dynamics, in both positive and negative ways.

TMC operations have three primary concerns:

1. Install and maintain CCTV equipment in the field and bring streams back to the TMC.
2. Control cameras in the field and use streams to guide operational decisions.
3. Share streams with partners, third parties, and the public.

IT concerns are intertwined with TMC concerns:

1. Provide, secure, and maintain network from the field to the TMC.
2. Provide and maintain systems that display and process CCTV streams at the TMC.
3. Secure and maintain outbound streaming to partners, third parties, and the public.



With CCTV stream sharing requiring close coordination between these two groups, two areas of focus should be addressed to ensure success:

1. **Field Equipment Connection to the TMC.** Successful coordinated approach will ensure that operations procure and deploy cameras and supporting infrastructure that satisfies needs and goals of IT while providing necessary capabilities for operations. This means early discussions of field equipment security, network segmentation that allows efficient and secure streaming at the TMC, and schedule or expectations for maintenance.

Lack of coordination can result in lack of mutual understanding, resulting in IT staff potentially structuring the network in a way that is overly restrictive, does not allow streams to easily flow to the TMC, does not provide necessary controls for TMC operators, or that may expose the TMC to security threats.

2. **TMC Connection to External Users.** While streaming from field equipment to the TMC tends to be a common activity and therefore is often a settled issue for most agencies, sending streams to external entities is a lot more challenging. By their nature, IT departments are wary of external entities accessing agency network and resources. Operations staffs often require different levels of access depending on their sharing partners, which makes network configuration, bandwidth, kill-switches, and other capabilities more complex. If IT and the operations teams don't coordinate and design the system together, TMCs risk building paths to share streams and developing policy documents just to find out that IT does not allow external connections.

A successful approach requires proactive communication between operations and IT personnel to ensure mutual understanding of requirements and capabilities and a clear plan for enabling external entities to securely access shared streams.

In addition to technical coordination between IT and operations staffs to ensure network and resources are setup properly, it is important for the two groups to coordinate during procurement efforts. If the IT department is responsible for procuring network infrastructure and equipment, without proper understanding and coordination for stream management and sharing, IT staff may procure equipment that is inefficient or incapable of handling the stream data load. Similarly, should operations staff procure a stream-sharing solution that requires custom stream processing and management equipment, if the interfaces between that equipment and existing IT equipment are not compatible, the agency may find itself wasting money and not gaining the expected performance or capability. Finally, existing IT staff may not be familiar with custom CCTV stream sharing equipment, and if the agency elects to manage the system internally, it may find that IT personnel are unable to troubleshoot or maintain the system.

In sum, the procurement process must consider both IT and operations needs in order to develop a unified approach to ensure proper equipment, services, and infrastructure are procured.

## **EQUIPMENT AND NETWORK MAINTENANCE**

Successful CCTV stream sharing requires a solid end-to-end solution. This means that each stream generated by the field camera must travel with minimum latency back to the TMC to be used by operators, and then shared out to external entities in a scalable way that does not impact the video stream's use in TMC operations. To achieve this, TMCs must procure, configure, operate, and actively maintain equipment and a network that support stream sharing.

Device and network configuration can vary in complexity depending on the age and diversity of field equipment and infrastructure, internal TMC needs, and desired stream sharing capabilities. If the agency is working with many different camera models and manufacturers and/or outdated camera equipment, the network and interfaces must support different transmission protocols, which makes the network and interface configuration more complicated.

For simple pan/tilt/zoom and video switching capabilities in the TMC, many agencies may use built-in advanced traffic management system (ATMS) functionality on their workstations. This means that incoming streams may be served to a set number of workstations and the configuration

can be simple, although often inflexible because the ATMS is built to do a lot of things and may not necessarily be capable of providing a rich set of features specific to CCTV management. On the other hand, some TMCs look for a more flexible framework and web-based CCTV management and operations approach that allow more flexibility to pull up and control many streams at the same time or to power large video walls. This type of configuration can be more complex as it may require additional equipment and internal TMC network bandwidth to distribute video among many thin clients in the center.

### *Thick vs. Thin Clients*

**Thin client:** designed to be small so that the bulk of the data processing occurs on a server someplace else.

**Thick client:** an application that performs the bulk of its data processing on its own (usually on your laptop or desktop computer)—relying less on servers someplace else.

TMC systems that rely on thick client CCTV management and streaming implementation often encounter larger challenges in sharing streams with external entities. Additional equipment is needed to move streams from the source through the TMC and out to external users. The network must be extended and secured, either using secure portals, so-called “demilitarized zones” (DMZs),<sup>3</sup> or similar network segments. In cases where the TMC is relying on more flexible thin client architecture, sharing streams externally can be simplified as external entities can be considered to be just another target output. In this configuration, changes may be limited to opening specific network paths or network segments to provide read-only access to streams.

Agencies approach these tasks in several different ways using:

1. In-house staff.
2. Onsite consultants.
3. Hosted solutions.

The in-house staff approach is common for agencies with a robust IT staff, especially in cases where IT and operations are actively collaborating on building the CCTV stream sharing solution. An in-house staff generally has a good understanding of the agency mission and constraints, which makes these individuals effective in maintaining and operating equipment and networks. One of the challenges in this environment is in cases where in-house personnel are maintaining proprietary equipment that they may not be familiar with. This requires continuous training and reliance on vendor support. A more common situation is that agencies have smaller IT departments or a weak relationship between IT and operations, which make in-house staff maintenance of equipment and network difficult or even impossible. In these cases, it is common to see agencies hire consultants who are integrated with TMC staff onsite.

The benefit of onsite consultant staff is that they are integrated in the TMC environment, while having support of the consulting firm and focused expertise. This means that if equipment changes or the network must be reconfigured to accommodate a new use case, the consulting firm may be able to provide resources and expertise specific to those needs. These consultants work closely with agency staff to define and implement solutions.

<sup>3</sup> In computing, a DMZ is a section of a network that exists between the intranet and a public network, such as the Internet, to protect an intranet from external access. By separating the intranet from hosts that can be accessed outside a local network (LAN), internal systems are protected from unauthorized access outside the network.

Finally, some agencies opt to outsource the entire solution to a contractor. The benefit of this approach is that the contractor is responsible for deploying equipment, maintaining it, and pulling streams into their system, with the TMC only needing a network connection to consume streams for operations purposes. The contractor handles the process of sharing streams with external entities without needing the agency to modify its network or deal with equipment maintenance. This model is a popular one in the tech world today. Cloud-based services are becoming a norm due to benefits of offloading all of the operations and maintenance challenges and maintaining flexibility to expand (or contract) services as needed. The obvious down side is the loss of some control and direct ownership of equipment. In most cases, for agencies without a strong, established IT department or consultant support, hosted solutions are ideal.

## CONTINUOUS SUPPORT REQUIREMENTS

Most TMCs are operating 24 hours per day, 7 days per week (24/7) to ensure coverage and response to congestion and incidents at any time. Some States may operate multiple TMCs with reduced but offsetting hours to achieve 24/7 coverage. Because of this coverage requirement, most ATMS functions and CCTV streaming are operational and supported 24/7. However, CCTV stream sharing is not always considered to be a critical function, especially in cases of constrained budgets and resources. As agencies realize the value of stream sharing with partners and third parties, the importance of maintaining stream exporting grows. Neighboring jurisdictions may be relying on shared streams to support their 24/7 operations. For example, local agencies may use incoming shared streams to adjust arterial signal system timing or activity in the middle of the night if there is a major incident that closes significant portions of the main State-operated thoroughfare.

TMCs approach 24/7 support of stream sharing differently depending on the size and complexity of their sharing system, staffing levels, expertise, and capacity.

- **No Support.** Some TMCs just do not have sufficient staff or budget to support 24/7 stream sharing. In these instances, if the stream sharing system goes down, partner agencies and third parties lose access to agency streams until regular work hours or appropriate staff is available to address the issue. The impacts are widespread, including the lack of coordinated response, potential for increased congestion and incidents, and overall loss of trust between partners.
- **Limited Support Using In-House Staff.** Agencies that realize the importance of 24/7 stream sharing but have staff or budget constraints may setup limited support arrangements. In these instances, staff may be on rotational on-call duty, or a vendor/consultant may be on-call to address critical issues after hours. The extent of this support may be addressing several typical and well defined issues, with any more complex issues being left to be handled during regular hours.
- **Continuous Support Using In-House Staff.** In-house, full, 24/7 support is usually set up during the development of a CCTV stream sharing solution. This support arrangement may include a team of dedicated internal or consultant staff that is trained or has necessary expertise to troubleshoot networks, equipment, and software used for sharing. This type of arrangement is not typical as the cost associated with training and securing on-call support in-house is high.



- **Hosted 24/7 Support.** As agencies are increasingly relying on hosted solutions, they are finding that one major benefit is inclusion of hosted 24/7 support. Hosted CCTV stream sharing systems are based on equipment and infrastructure owned and hosted by a dedicated service provider, and part of the provider solution includes 24/7 support of the equipment and systems. This means that if there is an issue with the system, the TMC may not even be aware as the failovers, load balancing, and hardware maintenance that may be occurring behind the scenes on the service provider’s side, but the streams continue to be available.

## LEGAL IMPLICATIONS

By its nature, surveillance capabilities bring a host of legal considerations agencies must address. Some of the primary legal considerations include handling of Freedom of Information Act (FOIA) requests for access to archived or realtime streams and appropriate use of surveillance equipment to preserve public privacy.

For the most part agencies have been able to address these challenges with respect to operating cameras for transportation operations purposes. To reduce cost and the challenge of responding to FOIA requests, many agencies have opted not to store or archive video streams. Those that do archive video may have specific staff responsible for responding to FOIA requests. Many TMCs define standard operating procedures (SOPs) that govern how operators use incoming CCTV streams. These SOPs usually specify permitted use scenarios focused on surveilling traffic flow, incidents, etc. In many instances, agencies also implement physical limitations to the field equipment to prevent cameras from being positioned in ways that provide a view into private residences or non-transportation related areas.

While agencies have managed these typical legal implications related to normal use for many years, the legal implications associated with stream sharing are newer and more complex. This complexity lies in relinquishing some control over stream usage once the streams leave the TMC network. Agencies do not have direct control over how streams are used by partners and third parties. To address these concerns, agencies rely on memoranda of understanding (MOUs), open agreements, and service charges.

### Memoranda of Understanding and Open Agreements

Agencies often develop MOUs with their sharing partners to support acceptable use and management of shared streams. MOUs vary in complexity but are generally meant to be simple and specific, allowing for quick agreement and limited protection when it comes to stream sharing. MOUs can address how shared streams can be used or specify unacceptable use of shared streams. While not typically legally binding, MOUs are a great tool to ensure mutual understanding between partner agencies while leveraging partner resources.

Open agreements are more formal in that they represent a contract whose terms do not constitute entire agreement between the sharing agency and its partners. Instead, open agreements may be focused specifically on CCTV stream sharing, where the agency wants to ensure it shares CCTV streams with its partners, but at the same time reserves the right to change the terms quickly to address any legal or privacy concerns.

MOUs and open agreements are sometimes accompanied by additional technical safeguards, such as specialized sharing portals and user or institutional permissions structures. For example, agencies may have MOUs with some partners and not others, or for some specific cameras and not others. To handle this, agencies may develop an access policy that specifies permissions that controls which cameras are shared with which partners. While these policies may require technical implementation, the real challenge is updating and maintaining the lists as cameras are added and removed and new sharing partners are included.

A number of agencies have noted that MOUs and other official agreements have been roadblocks to effective and open sharing. Almost any MOU or other agreement will require legal counsel to review the documents. This inevitably leads to delays, negotiations, and other issues that the two agencies signing the MOU need to work out. Additionally, some agreements may state that the signatory must agree to abide by the laws of a particular State. These types of agreements can kill multi-State video sharing efforts. (See the Virginia DOT Use Case in chapter 12 for a cautionary example of one such MOU).

### Concepts of Operations as a Replacement for an MOU

Because of the issues with MOUs and other agreements mentioned above, some agencies have opted simply to develop a Concept of Operation (ConOps) for how video sharing should occur. The ConOps is high level in its description of the philosophy of sharing and avoids any legally binding language. When agencies decide they want to share video data with one another, they simply agree (either in writing or via handshake) to agree to the principles of the ConOps. An example of one such ConOps responsible for a major multi-State, multi-agency CCTV sharing initiative can be found in appendix A.

### Service Charges

Most agencies do not charge their sharing partners for access to shared video feeds. This is to reduce barriers and encourage operational collaboration between agencies and agency partners. Many agencies also share their streams freely with third parties such as media and the public as part of the agency’s mission to keep the public informed of traffic conditions.

However, sharing costs and risks increase when sharing streams with external non-agency entities. Network access, large numbers of streams, stream quality, implementation of kill-switches, and other necessary adjustments for sharing with third parties introduces additional costs. While many agencies cover these costs as part of their operational budgets, others introduce fees for the streams sharing service to third parties. While the fees offset some of the cost of this implementation, the intent is not necessarily cost recovery.

The fee structure can take a couple of different forms:

1. **Flat fee.** This approach sets a flat fee to access TMC video streams for media and third parties that may be redistributing them or otherwise commercializing them. The fee is not meant to offset the cost of sharing, but is meant to provide commitment from feed consumers to use streams in a responsible manner and potentially add value.

- 2. HD stream fee.** This approach usually provides TMC video streams of average or low quality free to third parties. This quality is usually sufficient for most normal uses. In addition to the free feeds, the agency may offer access to higher quality or HD streams for a fee. This fee provides cost recovery for additional hardware and bandwidth necessary to generate and distribute higher quality feeds. Third parties that require high quality streams, such as media outlets, get the benefit of better-looking video for their broadcasts at a fairly low cost.

## MEDIA

The largest commercial consumers of TMC video streams are media outlets. TV and radio stations, especially in metropolitan areas, dedicate significant portions of their broadcasts to traffic updates. Morning and evening rush hours sometimes include traffic reports every 5-10 minutes. The market for this information is competitive, so media outlets are always looking for more and better information to share with their viewers and listeners. CCTV streams represent a great source of information for both TV and radio. TV news benefits from being able to not only observe live streams to get information, but also display those streams as part of their broadcast. People have significant visual capacity, and a quick 10-second live video of congestion, a lane closure, or road conditions can be sufficient for them to make commuting adjustments. As for radio, traffic reporters use a variety of information sources, including public and commercial traveler information websites, traveler calls to the station, public safety scanner radios, and, finally, streaming video. Streaming video can often provide more accurate and immediate information than any other sources of information.

Because media find such a great value and utility in streaming video, they are always looking for ways to obtain more streams at the lowest possible cost. Getting those streams from TMCs is a natural fit given the TMC's mission both to operate the system and inform its customers. Media pressure to obtain more streams has caused many agencies to consider stream sharing even if they did not see a use case for sharing with partner agencies. Once TMCs made basic streams available to the media, many TV outlets found that high-quality streams look sharper and more attractive as a component of the live telecast. One way the agencies make this offering available to the media is by investing in additional infrastructure and equipment to enable higher quality streaming. Given that this investment primarily benefits the media, agencies will often attach a price tag associated with providing these high-quality feeds. The cost does not always offset the investment, but it accomplishes two goals: 1) it reduces the cost of providing this service, and 2) it ensures that the service is limited to only those that truly require it or can assist the agency in achieving its goal of better informing its customers. In some instances, the cost and fee can cover the cost of installing and maintaining CCTV stream sharing equipment and infrastructure, and in rare cases generate some profit that can be reinvested in system improvements of the system to provide more and better quality streams.



---

## CHAPTER 6. TECHNICAL CONSIDERATIONS

---

Technical challenges associated with closed-circuit television (CCTV) streaming vary from transportation management center (TMC) to TMC based on the agency's information technology (IT) capabilities, network configuration and robustness, and system maturity. For most agencies, CCTV management is a core capability of their system, and expanding that capability to share those streams, while potentially costly and time consuming, is straightforward.

### NETWORKING

What sets video streaming apart from other data transfers at the TMC is that video streaming requires the transfer of significantly more data. The amount of data transferred varies based on the video resolution, compression algorithm, bitrate, etc. but can vary from a few megabytes (MB) to hundreds of MB per frame.

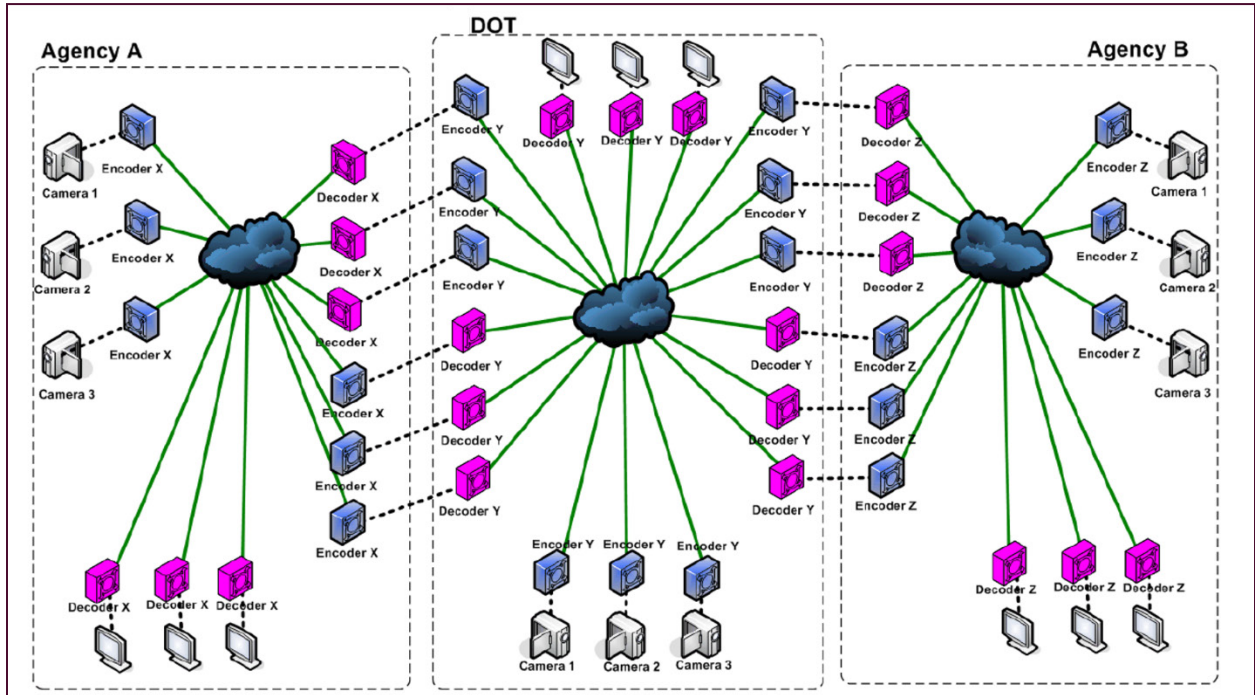
To make streaming video useful for TMC operations and for sharing partners and third parties, agencies must deploy and configure a flexible network that allows this massive amount of streaming data to be transferred while both keeping the network secure and reliable as well as ensuring that video quality is high enough to be useful.

Another related challenge TMCs face is that the network used to transfer streaming video from the field to the TMC and from TMC to sharing partners is usually the same network used to manage all other network traffic, such as advanced traffic management systems (ATMS) data transfers and general internet access. It is critically important to ensure that video stream sharing does not negatively impact the TMC's internal operations and communications.

### Network Configuration and Documentation

The first networking consideration in the context of video stream sharing is determining how the existing network is configured and documented. The agency network must connect to field cameras to allow streaming video to transfer from the field to the TMC. Once the streams are in the TMC, they are distributed internally for operational use and shared separately with third parties. There are multiple ways to configure the network to achieve this arrangement. An exhaustive list of potential configurations is outside the scope of this report given the endless variations in each agency's network equipment, network maturity, etc. However, several typical approaches are outlined here.

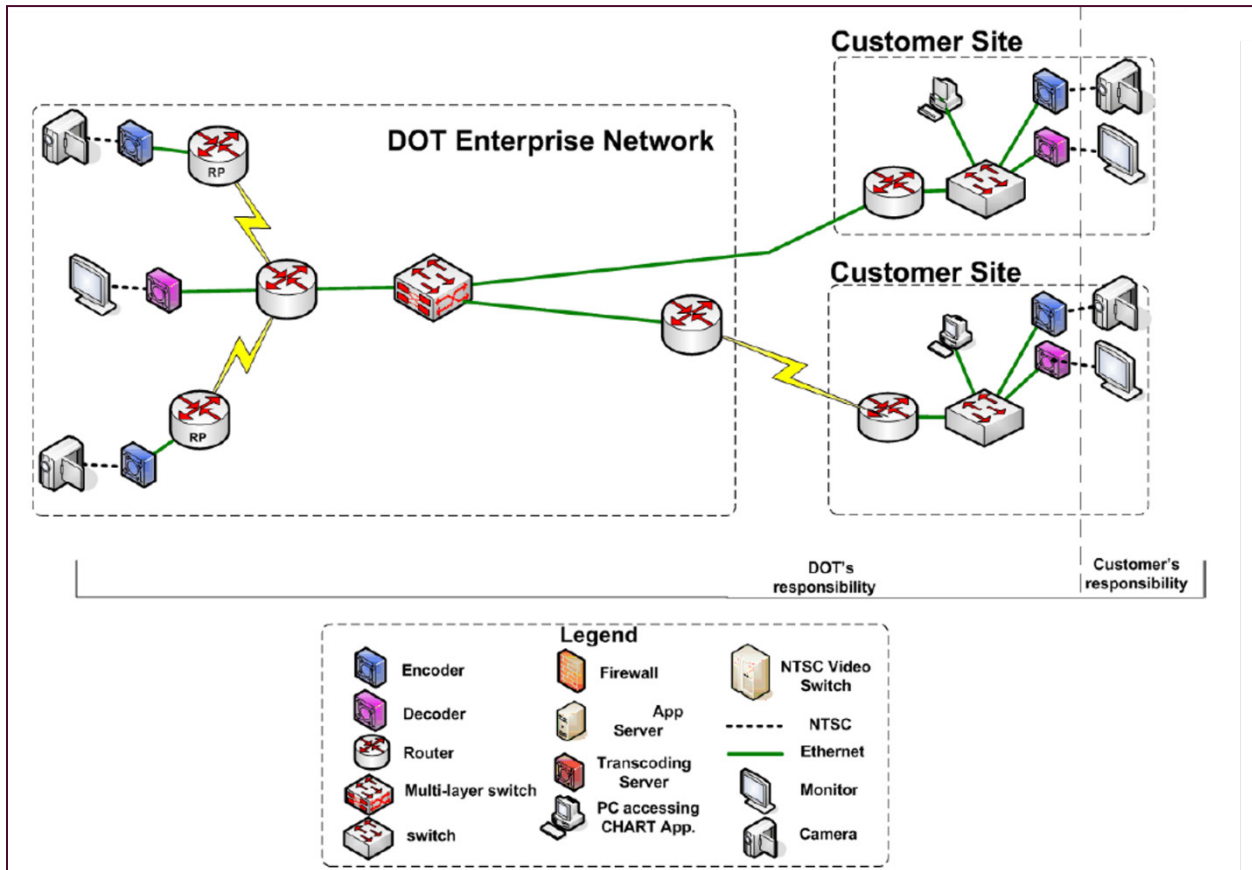
Many-to-many configuration addresses each sharing partner connection separately. For example, for a TMC to share video with Agency A requires deployment of a set of encoders at the TMC, decoders at Agency A, and a connection between these encoders and decoders. Similarly, if the TMC wants to share video streams with Agency B, it establishes another set of encoders, decoders, and connections.



© 2012 Maryland Department of Transportation, State Highway Administration

**Figure 4. Diagram. Example of an older many-to-many stream-sharing configuration.**  
 Source: CHART Submission for 2012 Digital State-Final, Maryland Department of Transportation, State Highway Administration.

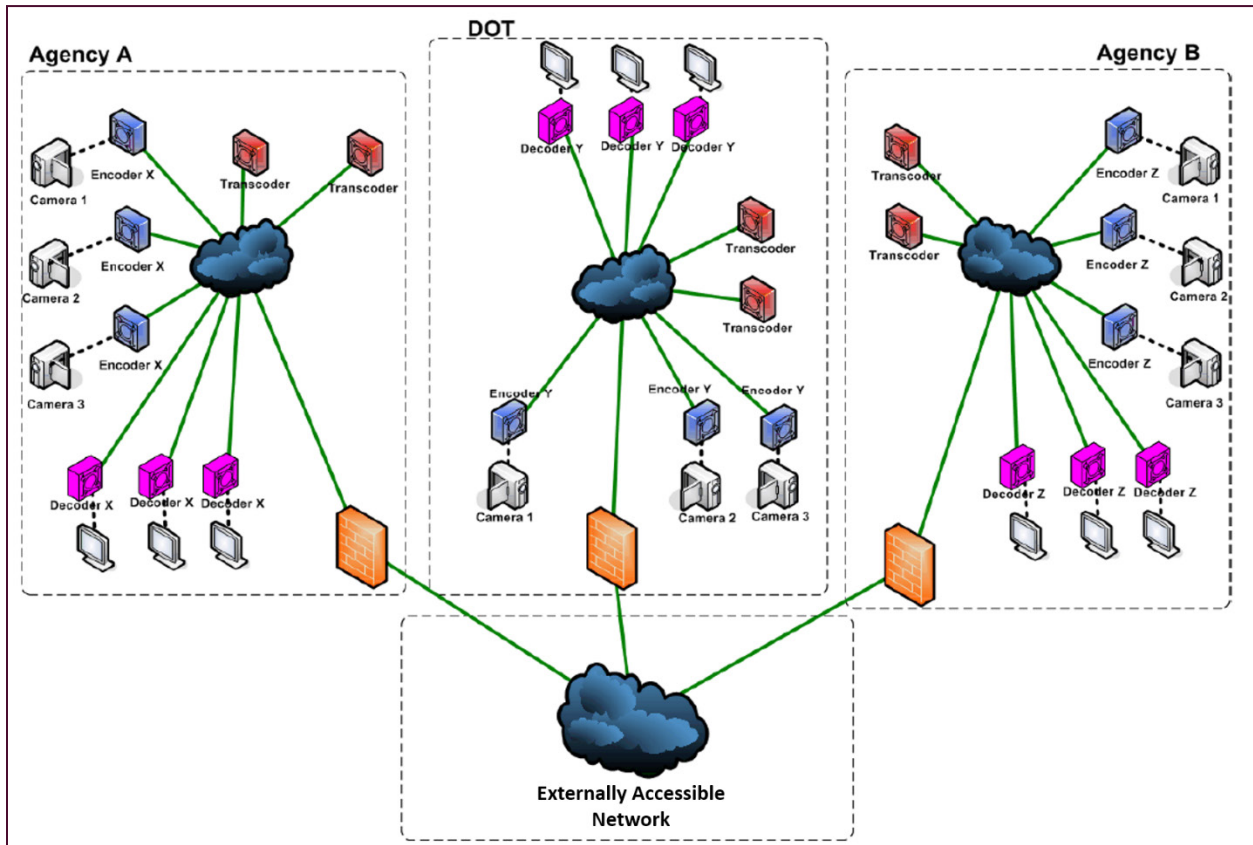
To support the many-to-many configuration, the network must be extended to reach across agencies. This can be accomplished several different ways, but one common way is to deploy agency network equipment to agency partner sites.



© 2012 Maryland Department of Transportation, State Highway Administration

**Figure 5. Diagram. Example of many-to-many network configuration.**  
 Source: CHART Submission for 2012 Digital State-Final, Maryland Department of Transportation, State Highway Administration.

The key challenges in this configuration is that it is not scalable because, with each new sharing partner, new equipment is installed in off-site locations, increasing both the cost and maintenance overhead. Security is not ideal because the many different potential entry points into the network will need to be maintained and patched regularly.



© 2012 Maryland Department of Transportation, State Highway Administration

**Figure 6. Diagram. Example of one-to-many stream-sharing configuration.**  
 Source: CHART Submission for 2012 Digital State-Final, Maryland Department of Transportation, State Highway Administration.

An alternative approach is to perform video encoding once inside the network and publish streams to a segmented network that is accessible to authorized third party sharing partners. This approach reduces the cost of hardware installation and deployment, while improving security by limiting network exposure to a single segmented part of the network.

Individual components of many-to-many or one-to-many models can be configured and deployed by internal IT and networking staff, or administered and managed by a consultant. Alternatively, some or all components of a stream sharing system can be offloaded to a hosting provider that takes responsibility of pulling in streams and building out network capability to share those streams among the agency and its sharing partners without modifying the agency’s existing network. This hosting model is becoming more popular due to lower maintenance overhead and a lower overall cost resulting from economies of scale.

Regardless of network configuration, it is critical for agencies to document their configuration to ensure overall understanding of network complexity. Changes to individual components of a network often have indiscernible and cascading impacts elsewhere in the network, with symptoms sometimes not appearing for a long time or until the network is compromised in some way. To avoid these negative impacts, agencies must document their network configuration and keep the



documentation relevant and up to date. Finally, stream sharing negotiations and MOUs are often easier when there is clear documentation of the network configuration that helps answer logistics and security questions.

## **Bandwidth Estimation**

Bandwidth represents the amount of data that can be sent across the network per unit of time and is usually measured in megabits per second (Mbps). Note that megabits (Mb) are not the same as megabytes (MB), which are generally used for measure of storage capacity (1 megabyte = 8 megabits or 1MB = 8Mb). Network bandwidth is a critical measure when it comes to video stream sharing since it is a direct limitation to how much video can be shared. For example, without any special configuration, a 100 Mbps network bandwidth means that it can handle up to roughly 65 standard definition streams at one time (given that stream resolution, quality, frame rate, etc. all impact data payload size). Note that this is a theoretical limit and the actual number of streams may be lower due to other variables such as network latency, network protocol overhead, other traffic on the network, etc.

Given the direct correlation between network bandwidth and stream sharing capability, it is critical for TMCs to accurately estimate bandwidth utilization and requirements before embarking on video stream sharing activities. Improper estimation can put the entire TMC network in jeopardy of becoming overloaded to the point where other critical operational capabilities are impacted.

If TMC operations and the video sharing network are sharing the same bandwidth, one approach to estimation is to analyze normal TMC operations bandwidth utilization to get baseline usage figures. Then, using the number of available camera streams, it is possible to estimate both average and peak utilization, which may be dependent on specific sharing solution implementation and number of sharing partners. The total necessary bandwidth would be the sum of the baseline TMC and peak stream sharing bandwidth. The key is to evaluate situations that may cause larger than normal demand on the network, such as major or long-lasting weather events, when sharing partners and the public may be more actively streaming feeds from multiple cameras in a region. If the bandwidth is estimated only based on average conditions, the TMC is at risk of having its network brought down during major events when camera streams are most valuable.

Bandwidth is impacted by multiple factors including Internet Service Provider (ISP) provided upstream and downstream (or upload and download) bandwidth, network switch ratings, firewall throughput, physical cable ratings, etc. This means that once bandwidth estimates are available, the TMC must ensure that all components of the network can support such bandwidth. If an ISP is providing 50Mbps/100Mbps up/down bandwidth, but key network components only support 1Mbps traffic, then the TMC will be unable to take advantage of all available bandwidth.

## **Latency**

Network latency is delay in communications across the network. Latency can be introduced in multiple places in the network. For example, poorly configured network switches or overly aggressive firewall packet inspections can introduce significant latency, which impacts the time it takes for data to reach its destination.

When it comes to video stream sharing, latency is usually the measure of how far behind from “live” video the stream is. This means that in terms of video stream sharing, latency is the delay between when the camera captures the video in the field and sharing partners see it on their screen. Latency can vary from a few seconds to half a minute or even longer. In addition to network configuration, video stream latency is impacted by the chosen streaming protocol. For example, HTTP Live Streaming (HLS) protocol focuses on high quality video but at the cost of high latency. This is because HLS prepares “chunks” of video and delivers them to the client for a smooth, high-quality video experience. The down side is that chunking of the video takes time (because of encoding, transcoding, buffering, etc.), so the video may not appear for 30-45 seconds after the camera captures it. Because of this, HLS is not ideal for realtime operational use by sharing partners. On the other hand, Web RealTime Communication (WebRTC) creates direct dynamic channels between peers without the need for any external encoders. This means that streams can be transferred with a very low latency, albeit with lower quality. However, this may be acceptable for sharing partners relying on video streams to react quickly to situations on the roadway even if the image is not perfectly clear.

In a race to reduce latency to achieve the necessary level of quality for TMCs, some transportation domain vendors are deploying proprietary protocols tailored for use in TMCs and for stream sharing with partners.

## SECURITY

Physical security and cybersecurity are critical considerations for TMCs as they look to share streaming video with their partners and public. Security concerns permeate all other aspects of TMC operations and video stream sharing specifically, including field equipment, network infrastructure and configuration, streaming and stream-sharing equipment, video players, etc.

Beyond physical security considerations for field cameras, the specific physical security considerations for stream sharing are with respect to equipment that may be deployed off-site or with hosted solutions. For example, a stream sharing architecture that depends on switches, routers, encoders, and decoders that is deployed off-site introduces risk in several areas. The off-site deployed equipment and hardware could be subject to compromise if the location does not have a strong physical security policy. This means that an unauthorized person could access physical equipment and either damage it or connect to it to either gain unauthorized access to video streams or modify its configuration to impact performance, ship video elsewhere, or compromise the upstream TMC network and gain unauthorized access to it. With hosted solutions, physical security is generally addressed as part of the policy, but still includes some level of risk that a person authorized to access physical equipment for one customer may also tamper (intentionally or unintentionally) with equipment for another customer.

Arguably, the more challenging security considerations are with cybersecurity. Any time devices are networked and connected, there is a risk of compromise on either end of the connection or by the man-in-the-middle (MITM) attack. While many of these risks can be managed and minimized in the context of internal operations through network security measures that prevent unauthorized access and control traffic within the network, the situation is more difficult to manage when certain portions of the network and its capabilities are exposed to shared streams with partners

and the public. For architectures requiring deployment of equipment at partner sites, the TMC must make external connections to each of the individual locations. To extend the network to these locations, the TMC must establish either private leased lines, which can be very expensive and not scalable to a large number of partners, or establish virtual private networks (VPN) that encrypt traffic to prevent anyone on the internet from having access to it. The challenge is that most VPN technology uses Transmission Control Protocol (TCP), which requires acknowledgment of each received packet of data in order. This increases network traffic and introduces additional delays in transmission. To address this, TMCs may have to consider a special Unigram Data Protocol (UDP) based VPN. Regardless of the type of VPN or secure connection with sharing partners, this model is not scalable, as an overly stretched network connecting to many different locations increases the potential for misconfiguration or the exposure of a vulnerability due to unpatched systems.

Another approach to this problem is to build an architecture that segments away the sharing portion of the network from the rest of the TMC network and secures that segment with an understanding that it is going to be accessed by many clients. Agencies can then implement specific cybersecurity strategies in that segment with appropriate fail-safe procedures that would prevent any compromise of the segment from impacting the TMC network and resources.

Hosted solutions often come with robust cybersecurity, as their focus is on video stream sharing and they can use their domain and cybersecurity expertise to ensure hardware, equipment, networks, and software are more secure.

Regardless of in-house or hosted solution approach, the two key points to remember are:

1. No networked system is ever 100 percent secure.
2. Regardless of money, time, and effort invested in developing cybersecurity technical solutions, humans are most often the cybersecurity weak link that enables a cybersecurity compromise. Staff and operators must be educated about cybersecurity risks and safeguards.

## VIDEO NORMALIZATION

When it comes to video stream sharing, it is critical to normalize video to allow it to be shared and managed more effectively. Video normalization refers to adjusting different parameters of the video stream to achieve maximum usability with the smallest video stream transfer cost and overhead. Most of the parameters used in normalization are interrelated, and improving one may have negative impact on others. The goal is to understand how the shared video streams are being used by partners and normalize streams to achieve those goals. For example, each sharing partner may have slightly different needs:

- Transportation agencies will look for average quality video with low latency to ensure situational awareness in near real time to support coordinated operations.
- Public safety agencies may be more concerned with very low latency video even if the quality is not great. This allows first responders to access video in the field in realtime and ensure their own safety and safety of others in the field.
- News media may be most concerned with high quality video even if it is delayed by 30 seconds because crystal clear visuals from the field have a bigger impact on the audience than

having true realtime information. Most of the time these streams are delayed anyway to allow kill switching video in case of incidents or other sensitive visuals that should not be broadcast.

- The public may be most concerned with having access to a large number of cameras on a public website, even if they are slightly delayed and lower quality, as they are looking for regional awareness or specific trip information.

Video stream normalization includes several key steps:

- **Compression.** Video compression is necessary to reduce the size of the video stream being transmitted. Compression can be achieved in a number of ways, such as by removing repetitive images and estimating motion changes. To achieve consistency across different camera technologies and stream types, TMCs can use specific compression algorithms for all their shared streams as part of video normalization. Some example compression formats include MPEG-4 Part 2, H.264 (aka MPEG-4 Part 10), H.265 (aka HEVC), etc.
- **Resolution.** Video stream resolution refers to height and width in pixels of a video being transmitted to the partners. Once again, to provide consistency across camera types and formats, TMCs normalize video streams to a specific resolution. Some standard resolutions are 240px (426 x 240), 360px (640 x 360), 480px (854 x 480, Standard Definition), 720px (1280 x 720), 1080px (1920 x 1080, High Definition), 4000px (3840 x 2160), but this can be customized as needed.
- **Frame Rate.** Frame rate refers to the number of video image frames displayed each second, and it is measured in units of frames per second (fps). Frame rate mainly impacts the smoothness of the video as a lower frame rate looks choppy and a higher frame rate looks smoother. This is because at a lower frame rate, the user is seeing fewer frames each second and the gaps between frames appear as choppiness of the video. Frame rate is important when visualizing high speed and detailed video streams, such as sporting events, but may not be critical for other uses. The standard frame rate is 24fps, but can vary from 1fps to 60fps, with most traffic cameras supporting up to 30fps.
- **Bitrate.** Bitrate represents the number of bits of data conveyed per unit of time in a video. Higher bitrate means that more information is available in each frame of the video and therefore the video looks to be higher “quality.” As with other variables, bitrate is related to the level of compression, resolution, and other factors. Bitrates range from 16 kilobits per second on the lowest end to over 1 gigabit per second for large uncompressed HD video on the high end. Bitrate limitations also exist on physical camera devices in the field. For stream sharing, bitrate is rarely considered in a vacuum and is instead adjusted in conjunction with other variables to achieve best quality at the lowest network cost.

When designing a video stream sharing solution, TMCs must consider their network limitations, partner agency needs, and all stream variables to create a normalized video to share with their partners and third parties. Normalization of video requires equipment, hardware, and codecs<sup>4</sup> to perform processing on incoming feeds before pushing them out to the sharing partners. Normalization introduces additional latency that needs to be properly communicated and understood by all parties in a sharing agreement.

<sup>4</sup> A codec is a device or program that compresses data to enable faster transmission and also decompresses received data.

## KILL-SWITCH TECHNOLOGY

The key TMC use case scenario for CCTV is to monitor traffic, detect and verify incidents, and coordinate response. In some instances, the field view may expose scenes that should not be shared with other entities. For example, a particularly graphic incident scene may be upsetting to the public and unnecessary for news media. At other times, specific security activity may be in the view of the camera, such as police enforcement activity or privileged movement of people or materials, and as such, should not be shared outside of the TMC.

When CCTV streams are pulled into the TMC, most of these use cases do not require any special treatment. However, when sharing streams outside of the TMC, operations staff must have the ability to abort stream sharing for individual streams in cases where the field situation may present a security issue or inappropriate information beyond operations. To achieve this, TMCs implement a “kill-switch” capability that ensures that each stream can be shut off at a moment’s notice.

While the concept is simple, implementation is not always so straightforward. Some of the key challenges include:

- Shutting off individual or sets of shared streams only based on impacted streams.
- Shutting off streams only to specific sharing partners. For example, a stream may be shut off for the public, media, and other TMC partners, but left available for public safety agencies or specific individuals that need the information to appropriately respond to the incident.
- Introducing artificial delay in shared streams to allow for sufficient time to activate the kill switch before that part of the stream is shared with others.

Sometimes TMCs only have the basic kill-switch capability that just shuts off all stream sharing paths. While potentially better than exposing undesired information, an all or nothing kill-switch is not ideal as it may impact coordinated response to important incidents where neighboring jurisdictions and operational partners are left blind to the situation.

## TECHNOLOGY AND INFRASTRUCTURE MAINTENANCE

CCTV technology, from actual cameras in the field to network infrastructure to sharing mechanisms, all change continuously to keep up with demands of both industry and the public. Streaming video has become commonplace with the proliferation of video services such as Netflix, Hulu, YouTube, and many others. To respond to this demand, manufacturers and developers continuously improve camera capabilities, compression algorithms, network capacity, processing power, etc. From the TMC standpoint, one of the challenges with such a fast-moving technology is keeping up with new devices, protocols, and needs. Agencies cannot afford to build an architecture that is not flexible enough to handle different formats and protocols. Instead, they are looking for ways to be technology and protocol agnostic. For example, with Flash technology end of life announced to occur in 2020, many Flash-based media players and stream distribution solutions will be going away. While the underlying protocols such as Realtime Messaging Protocol may remain in use, many others are being introduced to take advantage of newer web technologies and capabilities. This means that agencies must continue to adjust and provide video streams to their partners using the latest protocols to minimize network overhead and maximize shared stream quality.

In addition to software and protocols, vendors continuously update and market new cameras with new features and capabilities. While many cameras maintain backwards compatibility, the cost of backwards compatibility is high, and vendors tend to provide this compatibility for a limited amount of time. This technology evolution impacts stream normalization processes.

Another maintenance consideration is with changes in network infrastructure and equipment. Some agencies still rely on copper wire infrastructure, but more agencies are continuing to move to fiber optic networks, which provide many benefits. With the expansion of modern network infrastructure, agencies are also adopting more modern networking equipment, including the newest switches, firewalls, routes, etc. These changes can impact how streams are shared and may require frequent configuration changes to keep up with network changes. Similarly, as some agencies start relying more on hosted and cloud-based solutions, the cost and burden of maintenance is starting to shrink for many of the TMCs taking advantage of this new model.

---

## CHAPTER 7. HOW TO WORK WITH A SOLUTION PROVIDER

---

Successful closed-circuit television (CCTV) video stream sharing is predicated on a strong positive relationship between the agency and solution provider, especially in case of hosted solutions or solutions heavily dependent on continued involvement of the solution provider (vendor and/or consultant). This relationship must be built on mutual trust and understanding from the time the two parties connect to solve the problem of stream sharing. The agency is responsible for effectively communicating its needs, the solution provider for designing (or delivering) a solution tailored to those needs, and both are responsible for maintaining close collaboration for the duration of the relationship. Agencies should never feel bullied or beholden to the private sector, and vice versa. Usually the first opportunity to build this relationship comes before the Request for Proposals (RFP) development process.

With fast changing camera technology, network and streaming equipment and software, agencies often struggle to develop effective RFPs that will satisfy the key capabilities without being overly prescriptive. A typical RFP trap is collecting information from and about many different vendors and solution providers and then putting ALL of the capabilities into an RFP, making it impossible for any individual vendor or solution provider, or even a team of proposers to actually meet the requirements of the RFP. In these cases, RFPs outright fail to produce a winning proposal, or the winning proposer “stretches the truth” just enough to win the proposal only to disappoint with the inability to deliver, at which point it’s too late for the agency to back out or choose another option.

In order for an RFP to generate a successful outcome, it must be realistic and outcome based, rather than prescriptive and all encompassing. There are several key components necessary to write a successful RFP and select the right contractor.

### LANGUAGE IN THE REQUEST FOR PROPOSAL

- Strong definition of operational needs (ideally a well-developed Concept of Operations (ConOps)).
  - A well-developed ConOps allows the agency to define operational needs that are not focused on technology or solution, but rather operational needs and outcomes.
  - RFP describing operational needs allows proposers to determine how their capabilities can support those needs in a most effective way.
  - These operational needs should clearly cover expected cases including key differences in sharing needs as it pertains to partner agencies, public safety, media, and the public.
- Good understanding of the existing system and surrounding infrastructure.
  - Without understanding of the existing system and infrastructure, the RFP leaves proposers to guess the agency’s maturity. This can result in proposed solutions either being overkill or proposed costs being high to ensure the proposer is capable of handling the “worst case” scenario.
  - Instead, if the RFP effectively describes relevant network design, infrastructure, and existing equipment, proposers can provide a more tailored solution addressing needs in the given environment.

- List of key outcomes—not ways and methods to reach those outcomes.
  - Dictating type of equipment, approach, and even immediate output of the solution in the RFP can severely limit or even eliminate viable solutions.
  - A list of key outcomes separated from comprehensive list of capabilities allows proposers to focus on tailoring their solution to meet key outcomes, while understanding the context and environment in which this solution needs to be implemented.
- List of key constraints—budget, institutional, legal, etc.
  - Similar to outcomes, proposers must be aware of key constraints. This will prevent proposers and evaluators from wasting time exploring options that are not feasible.
  - Contractor Selection.

## CONTRACTOR SELECTION

- Appropriate expertise/support in evaluation of technical proposals.
  - One of the biggest challenges in evaluating technical proposals is understanding technical terminology and details of a proposed solution. The key is for the evaluating team to include both operations personnel and IT personnel to ensure the operational needs. In general, agencies should seek a partner that has expertise in every piece of the equation: networks, camera technologies, video encoding, etc.
- Data collection sheets.
  - A good contractor will have a pre-existing data collection/discovery sheet that can help the agency document its current operating environment. These data collection sheets help the agency and the contractor speak with one another in a common language. It also serves the purpose of aiding the contractor to understand the potential challenges and can help to provide a more accurate price estimate to the agency that is based off of real data rather than potentially incorrect assumptions.
- Contractor references.
  - The solution provider market place is not that large, which makes it feasible to rely on peer agencies to obtain references for proposing contractors. This is especially useful when agencies are similar in their CCTV technology and infrastructure maturity and have similar operational needs.
  - A contractor with a proven track record of delivering solutions that satisfy operational needs and willingness and flexibility to work with agency as a partner represents an ideal candidate.

The key themes in both drafting of the RFP as well as evaluation of the proposed solutions are as follows:

- Agency operations and information technology (IT) staff working together to create RFP and select a solution.
- Research and reliance on peers to learn about and evaluate solutions.
- Outcome focused efforts, not prescriptive or unattainable requirements.



## OPERATIONS

Once a winning proposer is contracted, it is critical for the agency operations and IT staff to remain engaged in a collaborative effort with the solution provider to ensure mutual understanding that leads to effective deployment, collaborative operation, and flexibility to remain on top of current technology trends and changes. These are marks of a true partnership rather than one where the agency tries to take advantage of the contractor with unreasonable demands, or the contractor tries to take advantage of the agency by delivering bare minimum or delivering a solution the contractor has rather than one the agency needs.

Transportation management centers (TMC) approach these relationships in different ways. Some opt to immerse contract staff in their TMC and make them part of the team. This approach is an effective way to establish clear communications channels and build expertise and capacity within the TMC to develop and manage stream sharing capabilities. Contract staff gets exposed to daily operational challenges at a TMC and can use their expertise to both troubleshoot immediate issues, but also learn about use cases and pain points that can guide improvements for the stream sharing solutions.

Alternatively, TMCs sometimes have the contractor or vendor design a solution and deploy the equipment, provide some initial training for the TMC staff, and then leave it up to TMC staff to run the system, with the only involvement being to troubleshoot major issues (often remotely) or provide proposals for additional capabilities as the TMC identifies additional needs.

In cases of hosted solutions, the contractor may be responsible for designing, deploying, and maintaining all of the infrastructure and services outside of the TMC. In these cases, contractors may have onsite personnel to develop understanding of usage patterns and needs and as an interface between TMC operations and IT staff, and the solution provider staff off-site.

### **Before and After Making an Award**

Before making an award (and even before writing an RFP) the agency should talk to other State and local DOTs who have already implemented CCTV sharing systems. The agency should talk to a broad group of agencies—not just three agencies that have implemented the exact same solution. This is the equivalent of checking the references of each of the potential private-sector providers. It is generally advisable to select a private sector provider that has a proven track record of delivering streaming CCTV video at the large enterprise level.



## CHAPTER 8. CAMERA AND COMMUNICATIONS EQUIPMENT

The types of cameras used by agencies can impact an agency’s streaming capabilities. It can also affect the desire for third-party access. Legacy cameras can be analog instead of digital/IP, and they can have different aspect ratios, lenses, and communication protocols—all of which can dramatically affect image quality, zoom capabilities, field of view, and the potential cost associated with streaming those camera feeds to third parties. Most consumer televisions are either HD or 4K resolution, and broadcasters want to deliver equivalent quality video to consumers. This means that these broadcasters typically desire a much higher quality of images than most agencies stream today. Figure 7 depicts 12 resolution types found in cameras and in consumer television monitors. Most legacy CCTV cameras output video towards the far lower left quadrant of this chart. Quarter Common Intermediate Format or QCIF (shown in the lower left corner) is what many legacy CCTV cameras broadcast—640 x 480px.

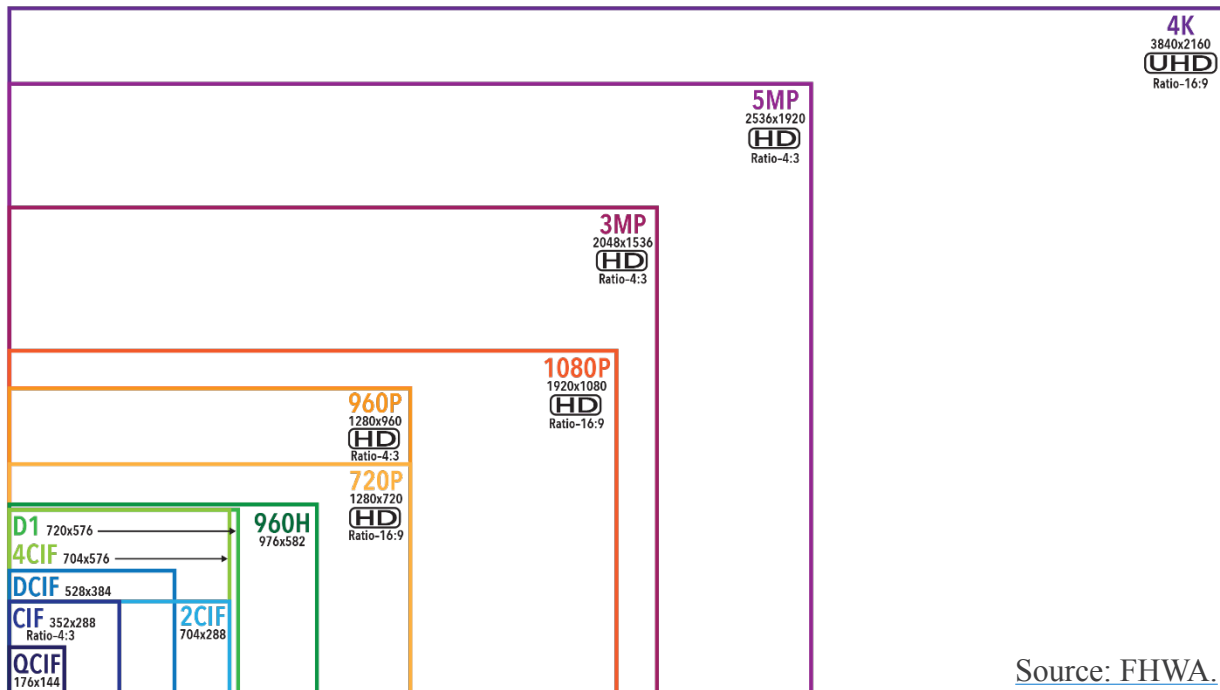


Figure 7. Illustration. Comparative resolution and aspect ratio chart.

IP camera resolutions can come in a wide variety of forms. Table 2 shows an example of the more common IP camera resolutions.

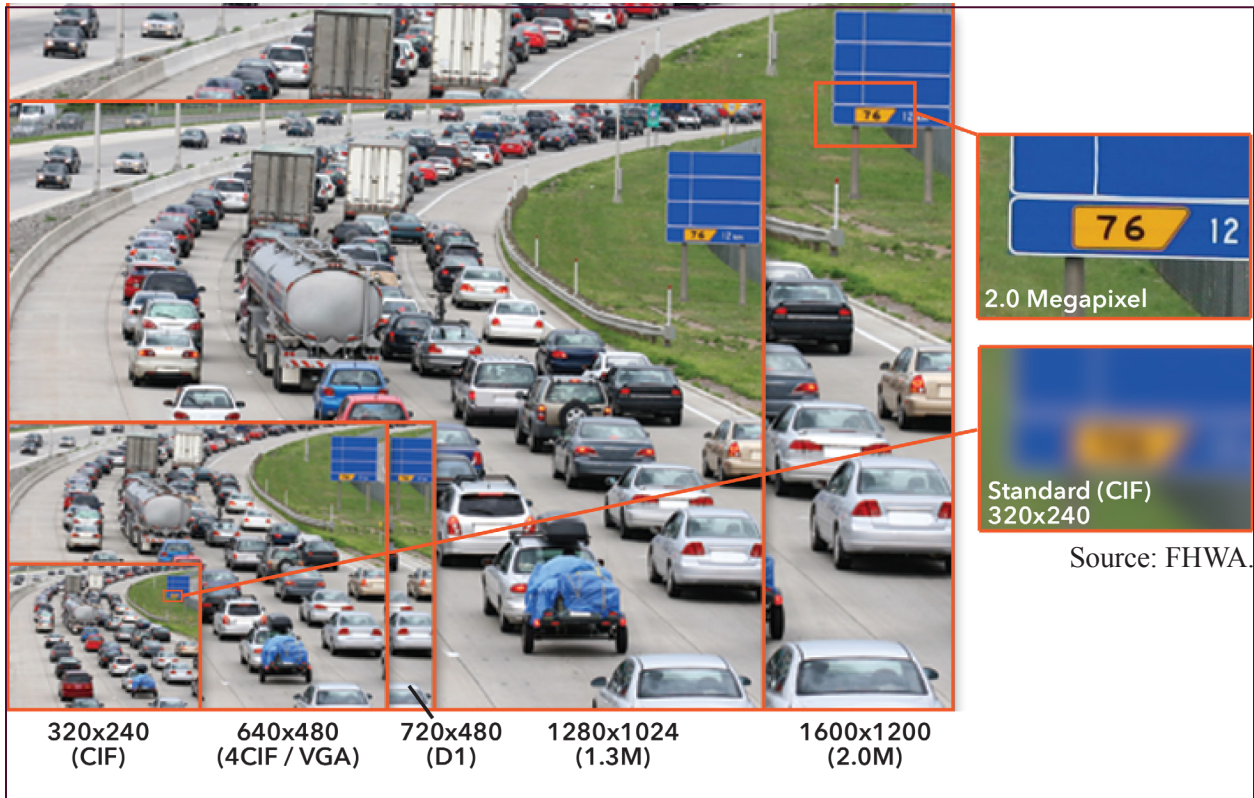
Table 2. IP Camera resolutions and megapixel equivalent.

Name	Horizontal Pixels	Vertical Pixels	Megapixel
CIF (Common Intermediate Format)	320	240	0.1
VGA (Video Graphics Array)	640	480	0.3

**Table 2. IP Camera resolutions and megapixel equivalent (continued).**

Name	Horizontal Pixels	Vertical Pixels	Megapixel
WVGA (WideVideo Graphics Array)	752	480	0.4
720P	1280	720	0.9
SXGA (Super Extended Graphics Array)	1280	1024	1.3
UXGA (Ultra Extended Graphics Array)	1600	1200	1.9
1080P	1920	1080	2.0
QXGA (Quantum Extended Graphics Array)	2048	1536	3.1
QSXGA (Quad Super Extended Graphics Array)	2560	2048	5.2

The higher the resolution of an agency’s CCTV camera, the greater potential value it will have to broadcasters and other stakeholders. Figure 8 shows how, at higher resolutions, greater detail can be detected in each frame of video—in this example, text printed on a highway sign can’t be seen at the lower resolution.



**Figure 8. Illustration. Resolution affects the quality of the video and determines what information can or cannot be detected.**

However, just because an agency has a high-resolution camera does not mean that the agency must rebroadcast its CCTV feed at the same resolution as is seen back at the TMC. Most streaming solutions will allow the agency to specify the format and resolution of the broadcast—thus saving the agency in bandwidth costs (if that is a concern). Some agencies make their lower-resolution streams available free of charge and only charge for higher resolution feeds to recoup increased networking costs. Others simply make the receiving agency or media outlet pay for a dedicated feed.

### Ideal IP Camera Specifications

IP cameras come in many types with many different specifications. Each specification can impact the eventual cost of rebroadcasting to third parties. To keep costs lower and to enable greater control over who ultimately can see the video feeds, agencies should replace older cameras with updated ones that support “independent multiple profiles concurrently.” Agencies should be aware that some camera manufacturers state that they support multiple profiles, but in practice, they only support *one* of the profiles at a time. This is particularly important when agencies want to maintain a high-resolution streaming capability for internal operations, but need to be able to simultaneously stream to third parties at a lower resolution.

Table 3 includes specifications that an IP camera must support in order to maximize capabilities and reduce costs. The camera(s) *must* support these parameters in a separate profile, which means the cameras must support multiple stream profiles.

**Table 3. IP Camera specifications that can enable lower-cost and more feature-rich CCTV streaming to stakeholders.**

Video	Description
<b>Video Compression</b>	H.264 sometimes referred to as MPEG4 Part 10 AVC (Advanced Video Coding).
<b>Resolutions</b>	Bare minimum target is CIF which is anywhere from 320 X 240 to 352 X 240 and others in this general range.
<b>Frame Rate</b>	Target is 15 fps (frames per second) Most specification sheets will give max numbers like 30 fps. This usually indicates “up to” which means they will support 15 frames per second.
Network	
<b>Protocols</b>	The preferred protocol is *RTSP (Real Time Streaming Protocol)
<b>Bandwidth or (Bit Rate)</b>	The target is 192 Kbps (Kilobits per second). Ensure that the camera supports adjustable/controllable bandwidth.
Multi-Profile Support	
<b>Separate Stream Profile Preferred</b>	It is preferred that cameras support separate streaming profiles to provide video to share without impacting the organization’s ability to provide internal video for its internal core mission.

## Emerging Features & Technologies

CCTV and IP Camera technologies are constantly evolving. Below are a list of current and emerging CCTV features that agencies may want to evaluate as they deploy new cameras or replace existing ones.

**Table 4. Emerging IP camera technologies beyond traditional transportation management center closed-circuit television camera capabilities.**

Technology	Why it might be useful
<b>HD or higher resolution cameras</b>	Higher resolution cameras enable more details to be gleaned from each camera—especially when the camera is a long distance from the roadway. HD resolution cameras can also provide greater coverage per camera at lower zoom levels.
<b>Ultra zoom lenses</b>	Ultra-zoom lenses allow for a single camera to cover a wide area at a great distance. For example, a camera can be placed high atop a radio or cell-phone tower or building and be located many miles away from the roadway while still providing for equivalent monitoring capabilities as a side-of-road camera. Attaching cameras to far-off locations can reduce costs as power and networking may be more readily available. A single camera with pan/tilt/zoom capabilities can also be leveraged to scan a wide area. Ultra-zoom lenses will need to be stabilized as small movements in the camera due to wind or vibrations can be exaggerated at high zoom levels.
<b>Innovative lenses</b>	Some camera manufacturers deploy fish-eye lenses or upwards facing lenses that look at cone-shaped mirrors. These lenses, when coupled with the right software, can allow for a stationary camera to provide virtual Pan/Tilt capabilities to multiple users at the same time—allowing two or more individuals to look in different directions.
<b>Finer control PTZ with zero drift</b>	Fine control PTZ cameras make zooming into and targeting incident locations easier. Most newer cameras also enable better position locking, which prevents the camera from drifting over time.
<b>Integrated Detection</b>	While more difficult to find on PTZ cameras, some manufacturers are rolling out embedded detection technologies in cameras that can detect anomalies, count vehicles, detect weather, etc.
<b>Low-light and no-light cameras</b>	Low and no-light cameras are a must for night operations. The newest cameras have advanced filtering and contrast control, which all but eliminate headlight glare and allow for night-time surveillance that comes much closer to typical daylight capabilities. These cameras can also help with other contrast issues at sunrise/sunset or going into or out of tunnels.
<b>Thermal cameras</b>	While still quite expensive, thermal imaging cameras offer the greatest night-time detection and monitoring capabilities of any camera technology today. They are also particularly useful for surveillance and infrastructure monitoring use-cases.
<b>Dual cameras</b>	Some agencies are deploying dual-camera technologies. For example, a single mount might include a standard HD color camera positioned directly next to a night-vision or thermal imaging camera.
<b>Orientation Sensors</b>	Most newer IP cameras can provide tilt and rotation data back to the TMC to allow the agency to map which direction (north, south, east, west, etc.) the camera is facing at any given time.

**Table 4. Emerging IP camera technologies beyond traditional transportation management center closed-circuit television camera capabilities (continued).**

<b>Technology</b>	<b>Why it might be useful</b>
<b>Mobile Cameras</b>	Several agencies are now deploying mobile PTZ cameras to the top of their Service Patrol and/or maintenance vehicles. When coupled with in-vehicle streaming solutions, these mobile CCTV assets can allow TMC operators boots on the ground viewing capabilities.
<b>Camera/Sensor integration</b>	A few manufacturers are now integrating additional sensors into cameras— understanding that some agencies may want to deploy more capabilities at each site. For example, some manufacturers may integrate CCTV cameras into RWIS stations, Doppler radar, pavement temperature sensors, etc.





## CHAPTER 9. BUSINESS PRACTICES AND POLICIES

---

This section examines the different business approaches to video stream sharing including:

- Free access for all.
- Reciprocal access.
- Tiered access (i.e., free for public, fee for higher quality video for media).
- Cost recovery model.
- Profit model.

This section will give detailed examples of how each business practice works, providing agency examples/use-cases where available. The pros and cons of each business practice will be discussed along with details as to how agency policies may impact the success of each practice.

### FREE ACCESS

Free access approach is the most liberal approach to closed-circuit television (CCTV) stream sharing. This approach is based on the concept that sharing of CCTV streams provides significant value to the end customer – traveling public – through improved safety and mobility resulting in more efficient and effective operations and coordination. The agency’s core mission is to serve the general public and providing CCTV sharing capability speaks directly to this core mission. A free access approach is more attainable for agencies that have already made an investment in field equipment and infrastructure, and need to make smaller incremental investments to make this data available to third parties.

To support free access, agencies must budget for implementation of CCTV sharing mechanisms, as well as on-going operation and maintenance of supporting systems. These funds can be secured and allocated as part of transportation management center (TMC) operational budgets. To make a case for budgeting of CCTV stream sharing, it is critical for the agency to show benefits to operations and to the public. From a “political” standpoint, free access provides exposure via the media and other outlets that provide a positive image for the agency in the eyes of the legislators, the public, and sharing partners. Similarly, free access allows smaller local agencies to become more engaged in managing of transportation issues providing additional benefit to the TMC and the public. For example, a public school system may benefit by gaining awareness of traffic conditions from shared video feeds and adjust schedules and routes accordingly.

### RECIPROCAL ACCESS

Free access for all is not always feasible or possible, especially for agencies that do not have robust infrastructure and sharing capabilities. However, as a step towards a free access goal, agencies sometimes begin by developing sharing capabilities with partners that may be able to share their own video streams (or other data) of value with the TMC. For example, a State or local department of transportation (DOT) responsible for managing an urban network may benefit from access to public safety surveillance equipment to augment TMC capabilities and situational awareness.

In exchange for access to those cameras, the State or local DOT may offer to share traffic cameras with public safety partner(s) in that urban area. The implementation of these individual reciprocal sharing mechanisms can be used as a piecemeal approach to building a more robust sharing solution that can become a free access for all in the future. In the meantime, it presents an opportunity to make a case for sharing to the decision makers and identify other potential partners looking to strike a reciprocal deal.

## TIERED ACCESS

Free access for all is a good approach, but sometimes suffers from the lowest common denominator problem. Because agencies must make sure they are able to share effectively with everyone, they may select the sharing mechanism that ensures the underlying network and sharing solution doesn't crash or that the costs don't balloon beyond what the agency is capable of absorbing. This often means that everyone gets average or low-quality video access – the lowest common denominator. It may also mean that in case of an incident, a kill switch is engaged shutting off access to all – the public, media, and operational partners. This can be counterproductive as the operational partners may present most value in cases of major incidents as they can provide support or coordinated response. Similarly, the media outlets may decide that low quality video is not good enough to use during live broadcasts, further limiting traveler information dissemination and value of the agency's CCTV sharing investment.

A way to address these issues is to implement a tiered access. Tiered access can be based on video quality and/or quantity. Some of the common approaches include the following tiers:

- 1. Operational Partners Access (Free)**
  - a. Medium to high quality video, sufficient to assess the situation and respond accordingly.
  - b. Medium to large number of video feeds ensuring adequate coverage of a larger region to support regional coordination and cooperation.
- 2. Public Safety (Free or \$)**
  - a. Medium quality, low-latency video providing close to realtime access to ensure safety of first responders and those on the scene.
  - b. Access to several feeds at a time to support specific incident response.
- 3. Media (\$\$\$)**
  - a. High quality, sometimes higher latency video that provides a view that looks good during live broadcasts.
  - b. Usually access to one or two feeds at the time as broadcasters often display a single video view supporting narrative for each geographic location in the traffic report.
- 4. Public (Free)**
  - a. Low quality, higher latency video that allows adequate view for general public looking to get better informed about conditions on the roadway.
  - b. High number of video streams available to support public use cases such as viewing cameras along an entire route.

## **COST RECOVERY MODEL**

The cost recovery model is most often implemented by agencies that realize the value of CCTV video stream sharing, but have limited or no funds to implement the sharing mechanism. To achieve the goal of sharing, these agencies may evaluate costs associated with design, deployment, and operation of the stream sharing system and pass that cost along to sharing partners. The idea is that the agency still provides value to sharing partners and the public by sharing the CCTV video streams, even if the agency has no dedicated funds to support the sharing efforts.

The main drawback of this approach is that it limits the number of sharing partners willing to invest. If the value to sharing partners is marginal, they may not be willing to foot the bill alone. The economies of scale sometimes make the cost acceptable as the number of sharing partners increases, but to reach this level, the agency must make its own initial investment, which may be challenging.

## **PROFIT MODEL**

While the profit model is not pervasive across public agencies, it does appear in some instances. The approach here is similar to the cost recovery model, except that the sharing partners incur higher cost to consume agency video than what it costs the agency to share that video. The idea behind this approach is that the agency has made an investment into a system and can use profits to reinvest into that solution and continue to build out capabilities, improve stream quality, maintain a more stable and robust sharing infrastructure, and keep up with the changing technology. This approach makes sense for high value CCTV deployments along corridors that may experience high levels of congestion and/or incidents where sharing partners may benefit from the information coming from those cameras and media may be making significant profits from advertising or other sponsorships associated with live broadcasts that utilize shared TMC video streams.



## CHAPTER 10. RECOMMENDATIONS

---

Deploying a streaming video solution is technically fairly simple. However, developing a long-term plan for operations and maintenance of the system is a task in and of itself. Agencies that can sustain and grow their systems for years to come will have tackled the following tasks:

- a. They will have fully documented the benefits of sharing streaming video with stakeholders, and will routinely communicate the various business cases for doing so on a regular basis to staff and stakeholders.
- b. They will engage stakeholders on a regular basis to ensure that needs are being met.
- c. They will have implemented processes that make it easy for new stakeholders to share or receive video feeds without having to change their own networks or sign restrictive agreements.
- d. They will publicize their video sharing efforts frequently to legislators, the media, and other stakeholders.

The following is a summary of recommendations and lessons learned that have been gathered during this synthesis. Agencies should focus on these key considerations to help ensure long-term success, agency buy-in, and minimal disruption to operators and budgets.

### **BUSINESS CASE JUSTIFICATION**

To be successful in sharing closed-circuit television (CCTV) video streams, key leaders within the agency must identify and agree upon the overall benefits of sharing CCTV. This is critical to justify the necessary investment and effort. The key benefits to the agency include things like: Improved incident response, improved relationships with partners, better cross-jurisdictional coordination, more effective traveler information, and public service. Agencies that understand these benefits are better able to provide long-term budget justification for continued streaming.

### **Operational Considerations**

Agencies can minimize the impact on operators by implementing easily accessible kill-switches built in to the agencies advanced transportation management system (ATMS) and CCTV platform. Kill-switches reduce operator concerns over zooming in to sensitive incidents. The most technically mature agencies have implemented kill-switches that only disable video streaming to the public and the media while continuing to stream to public safety and other agency partners.

## Technical Considerations

While there are many feasible technical solutions to video streaming, the most successful, cost-effective, and stable solutions follow these guiding principles:

- They leverage existing, proven technologies.
- They avoid motion jpeg technologies or providers who specialize in similar outdated technologies.
- They invest in enterprise level management that provides the following basic features:
  - Normalization—they normalize different video feeds from various camera technologies. They handle compression, color, resolution, frame rates, quality, and output formats.
  - Streaming—they are capable of high-volume, low latency, and one-to-many streaming.
  - Manage—they provide tools that make it easy for agencies to manage their streams, application programming interfaces (APIs), statistics, update metadata, and otherwise manage and trouble-shoot streams.
  - Share—they provide for multiple sharing options including browser-based, mobile, thick client, etc.
- They work with companies that have expertise in the multiple aspects of video sharing (networking, standards, etc.) that can dramatically affect cost.

Regarding hardware, agencies should always replace failing cameras with newer IP streaming cameras that support multiple, simultaneous profiles. This specification will make it easier to stream video to different “Classes” of users—the media, public, and trusted agencies—with minimal impacts on operators, networks, cost, etc. More detailed hardware specifications can be found in Table 3.

## Concepts of Operations vs. Memoranda of Understanding

While memoranda of understanding (MOU) are popular with agencies, they can be problematic. Agencies that must develop a MOU should avoid “governing” language, which can inhibit cross-border sharing. Other constricting language that moves the MOU closer to a contract should also be avoided.

The most open and successful sharing strategies do not involve MOUs or legal agreements at all. Instead, they focus on common operating principles (or a concept of operations (ConOps)) that explains the overarching goals of sharing.

A well-defined ConOps will communicate the need, purpose, and vision of video streaming both within an agency and among partners. A strong ConOps will address issues of performance expectations including uptime, network utilization, as well as clear case for controlled sharing in case of sensitive information during incidents – such as kill-switches and PTZ control.

## **Institutional Considerations**

The key to successful stream sharing starts within an agency. Close coordination between agency information technology (IT) and operations staffs is extremely important as it provides a strong base for development of good relationships with external partners. A strong ConOps can be an ideal way to establish strong relationships with external partners without overhead that sometimes comes with MOUs or other formal agreements.

While in-house implementation is a good approach in some instances, agencies have benefited from leveraging expertise of their private sector partners who can provide expert installation and maintenance as well as continuous (24 hours per day, 7 days per week) operations. In fact, hosted solutions have become more prevalent among agencies due to their lower cost and higher reliability bought on by the ability to leverage economies of scale. Agencies now have the option of purchasing hardware appliances that support the streaming of hundreds or thousands of cameras OR they can outsource their streaming entirely.

Agencies need to strongly consider the increased burden on staff who will need to manage technology, networks, and media/third party relationships.





## CHAPTER 11. USE CASES

Below are several State department of transportation (DOT) use-cases outlining different approaches to closed-circuit television (CCTV) video stream sharing from Maryland, North Carolina, and Virginia. Key differentiators between each user-case include:

**Table 5. Highlights from three State agency approaches to streaming video.**

State/Agency	Key Highlights
<b>Maryland</b>	<ul style="list-style-type: none"> <li>• Developed a streaming solution that has since been adopted by other States and agencies around the country.</li> <li>• Provides free and open access to thousands of camera feeds.</li> <li>• Handles different camera types, resolutions, etc.</li> <li>• Provides a consistent way to connect to agency video without the need for unique or additional hardware.</li> <li>• Technical solution developed by the private sector (Skyline Technology Solutions).</li> <li>• Solution currently consolidates over 12,000 streams from the National Capital Region.</li> <li>• ConOps focused—not MOU/legal agreement focused.</li> </ul>
<b>North Carolina</b>	<ul style="list-style-type: none"> <li>• Innovative approach to working with the media in terms of paying for the required hardware.</li> <li>• Innovative approach to receiving additional non-financial benefits to the State through the provision of air-time.</li> </ul>
<b>Virginia</b>	<ul style="list-style-type: none"> <li>• An outsourced approach to the technical, management, and licensing agreement solution.</li> <li>• Licensing managed by Iteris.</li> <li>• Technical solution implemented by Skyline Technology Solutions.</li> <li>• Has consolidated video with data.</li> <li>• Has a more restrictive MOU that makes it more difficult to share video streams with government entities operating outside of the State of Virginia.</li> </ul>

ConOps = concept of operations. MOU = memorandum of understanding

### MARYLAND DEPARTMENT OF TRANSPORTATION

The Maryland DOT’s transportation management center (TMC) has been providing video feeds from its traffic cameras to multiple departments, agencies, key decision makers, and the public since the late 1980s. They have always architected their streaming solutions throughout the years in a way that allows them to restrict access to those feeds “on the fly” to protect sensitive footage

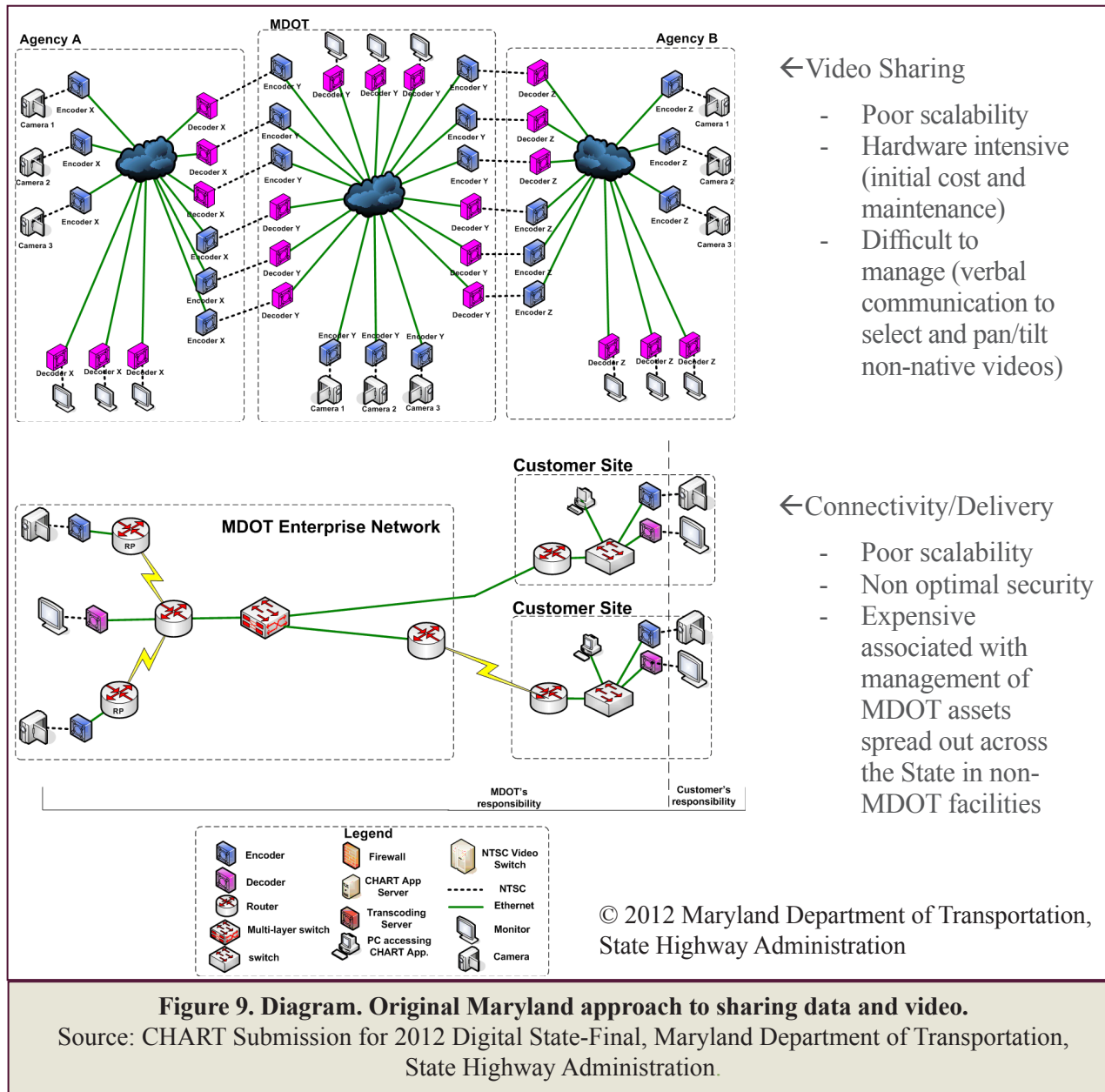
during critical events. However, in the late 2000’s, the agency was given a mandate to further increase the ability to share live video with more public safety agencies, other States, the public, and the media while also being able to ingest additional video feeds from these partners. With this new mandate, the Maryland DOT faced three main obstacles:

1. The variety of the native video formats made interoperability difficult;
2. The high bandwidth of the native video feeds restricted scalable distribution across networks; and
3. The inability to share video in a common format across network, to large distributed user groups, as well as mobile responders.

To reach the highest number of non-DOT "public" first responders in Maryland, the Coordinated Highway Action Response Team (CHART) immediately involved the Maryland Department of Information Technology to ensure that the State’s intranet (networkMaryland) would be able to serve as an additional conduit of the Maryland DOT emergency data and video system.

The work itself consisted of two primary tasks. If data and video was to be shared, the first task was to establish a secure video and data distribution architecture. The second task was to establish a scalable solution for transcoding the source video formats into a common format to enable multiple centers to view video and data from multiple agencies.

**The problem:** As shown on the top half of figure 9, in the past, data interoperability was met by placing “dedicated workstations” in each other’s facilities and video interoperability by encoding/decoding/re-encoding/re-decoding video.

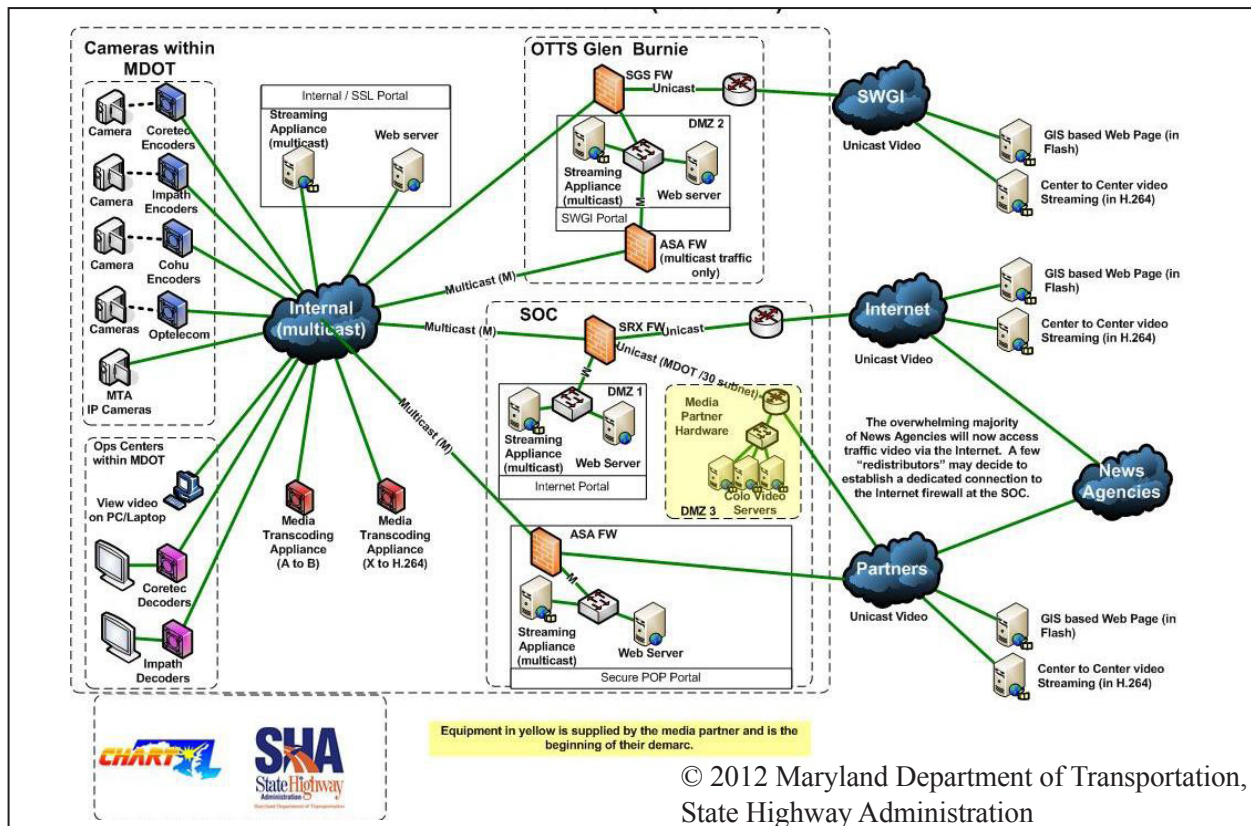


**Figure 9. Diagram. Original Maryland approach to sharing data and video.**

Source: CHART Submission for 2012 Digital State-Final, Maryland Department of Transportation, State Highway Administration.

**The Solution:**

- Video shared with partners through security approved, thoroughly tested Commercial Off the firewalls.
- Video translated between IP-based formats instead of re-encoding/re-decoding between NTSC.
- Multiple Security zones to enable sharing (and non-sharing when necessary) by class of video user.



**Figure 10. New Maryland architecture: sharing video and data across multiple security zones.**  
 Source: CHART Submission for 2012 Digital State-Final, Maryland Department of Transportation, State Highway Administration.

MDOT’s technical solution was ultimately implemented by Skyline Technology Solutions which also implements enterprise-level video sharing solutions to other States. MDOT is successfully sharing thousands of video feeds from multiple agencies utilizing various source video formats by transcoding the video in real time, reducing the bandwidth of the video, eliminating unnecessary equipment, and presenting it in a common format that is network, security and distribution friendly. As a result, CHART has been able to increase the number of cameras available to the public as well as provide increased situational awareness to decision makers across the State.

Maryland has worked to replace aging cameras with newer IP cameras that can stream to multiple, simultaneous profiles. Maryland has also invested heavily in mobile CCTV cameras. These cameras can be mounted inside the vehicle dash or mounted to the top of the patrol vehicle with an integrated PTZ feature that can be controlled remotely at the operations center. Each patrol mounted camera costs approximately \$15k to install and can be controlled by the State’s transportation operation center/transportation management center (TOC/TMC) software. Video is transmitted via the State’s secure Access Point Name (APN) across an AT&T network. These cameras provides agencies with mobile, remote live streaming video, providing realtime views of incidents and events where there are no fixed mounted cameras or infrastructure to provide surveillance. Now, operators and managers in the operations center have more information available to respond and manage planned and unplanned events. The State freely streams their mobile CCTV cameras to other agencies and partners.



© 2016 Maryland Department of Transportation, State Highway Administration

**Figure 11. Photo. Example of MDOT’s Service Patrol Mounted CCTV camera.**  
Source: CHART Presentation to Ops Academy – 2016, Maryland Department of Transportation, State Highway Administration.



© 2018 University of Maryland Center for Advanced Transportation Technology Laboratory

**Figure 12. Photos. Compound figure depicts four examples of on-scene video captured from mobile streaming CCTV cameras mounted in or on service patrol vehicles.**  
Source: RITIS Website - MATOC Screenshots.

## NORTH CAROLINA DEPARTMENT OF TRANSPORTATION

North Carolina Department of Transportation (NCDOT) does not currently have the technical capability to stream their 900 CCTV cameras to the public or web at this time. They only publish shapshots to their traveler information website; however, they do allow the media to install servers in their TMCs to get access to live video streams.

NCDOT has created a unique method of funding their media-sharing. First, they make the media pay for and install their own equipment at the NCDOT. This arrangement is non-exclusive in that the NCDOT retains the right to enter into multiple agreements with other media entities—also requiring that those additional parties bear the cost of providing their own equipment. Alternatively, the media outlets can join forces and equally share the cost of providing images and equipment through additional agreements (see figure 13).

2. The parties acknowledge the need to purchase, install, and maintain equipment and infrastructure in order to accomplish the purpose of this Agreement.

A. NCDOT will provide the necessary equipment to convey the CCTV images from within the **Piedmont Triad Regional Traffic Management Center** to a reasonable location, agreed upon between the NCDOT and the USER, where the USER can access the images.

B. The NCDOT and the USER shall agree upon the type and location of USER's equipment, including transmission equipment, a structure to house said equipment within, logistics of access to said equipment and any other issues of concern in a written addendum to this Agreement signed by all parties. All equipment supplied by USER pursuant to this agreement shall at all times remain the property of the USER. USER shall be responsible for operating and maintaining its equipment at USER's expense.

3. NCDOT has the right to allow additional parties' access to the Video Images. Additional parties may

A. enter into a separate agreement with NCDOT and bear costs of providing their own user equipment, or

B. equally share the cost of providing image distribution amplifying equipment and its housing with the existing users. USER and additional users shall furnish NCDOT an executed legal agreement stating that the additional user has paid the pro rata costs to the existing users and is bound to the terms of this Agreement prior to receiving Video Images via the USER's equipment. Each user shall be responsible for providing its own transmission equipment.

The USER agrees not to give, sell or otherwise provide Video Images to additional third parties that have not satisfied the above requirements, unless that party is owned by or affiliated with the USER, without requesting and receiving permission from NCDOT.

If any party's access to the Video Images is terminated, the terminated party shall forfeit the invested pro rata payment to the existing user(s).

USER's equipment shall not adversely affect the NCDOT's equipment. NCDOT's equipment shall not adversely affect USER's equipment.

© 2019 North Carolina Department of Transportation

**Figure 13. Illustration. North Carolina Department of Transportation media agreement cost language.**

Source: Agreement between NCDOT and media, North Carolina Department of Transportation. n.d. "Media Agreement." last accessed, May 1, 2019.

Additionally, the media are required to provide NCDOT with “15 thirty (30) second Public Service Announcement spots each year” that will run between the hours of 6AM and 7PM as shown in their Media Agreement in figure 14.

NCDOT is also in the middle of a massive infrastructure upgrade to all digital video and a transition to a new network. After the completion of this upgrade, NCDOT plans to re-evaluate, and eventually deploy streaming video. The North Carolina legislature is even considering recording their live traffic feeds for safety and security reasons.<sup>5</sup> A \$1.5M bill<sup>6</sup> has been put forward to their general assembly.

5. USER agrees to acknowledge NCDOT for providing Video Images by adding logos and text during use of Video Images. NCDOT and the USER shall jointly develop the logos and the format of any text, provided that any such logos or text must be of broadcast quality and must comply with the USER’s reasonable rules and regulations.

USER agrees to provide NCDOT

A. 15 thirty (30) second Public Service Announcement spots each year. These spots will run between 6 AM and 7 PM.

B. Up to 3 logo changes per year at NCDOT’s request.

6. NCDOT agree to provide live Video Images when these images are generated. Except as provided below, the USER has complete discretion in deciding which Video Images to use:

A. NCDOT and the USER acknowledge that the Video Images likely will feature members of the general public and that the law extends to members of the general public certain rights of privacy. The USER hereby agrees that any use it makes of any Video Images shall be consistent with the right of privacy as defined by law. Nothing contained herein shall be construed to prohibit the USER from broadcasting any Video Images that are bona fide news stories provided that any such use shall be consistent with NCDOT’s and the USER’s legal obligations.

B. The USER shall not broadcast any Video Images that NCDOT and the USER reasonably believe contain images that are inappropriate for public view.

C. If the Video Images are unavailable due to ongoing response to emergency situations, technical difficulties, maintenance, or any other reason, NCDOT shall not be responsible for providing the USER with replacement content during such period of unavailability; provided, however that if such periods of unavailability become so frequent or of such a long duration that, in USER’s discretion, the purpose of this Agreement has been materially impaired, then USER may terminate this Agreement immediately upon notice to NCDOT.

D. The USER understands and agrees that the Video Images are provided to USER to inform the public about traffic conditions in the Greensboro and Winston Salem areas. Except as set forth herein, the USER shall not use such images for any other purpose without the written consent of NCDOT.

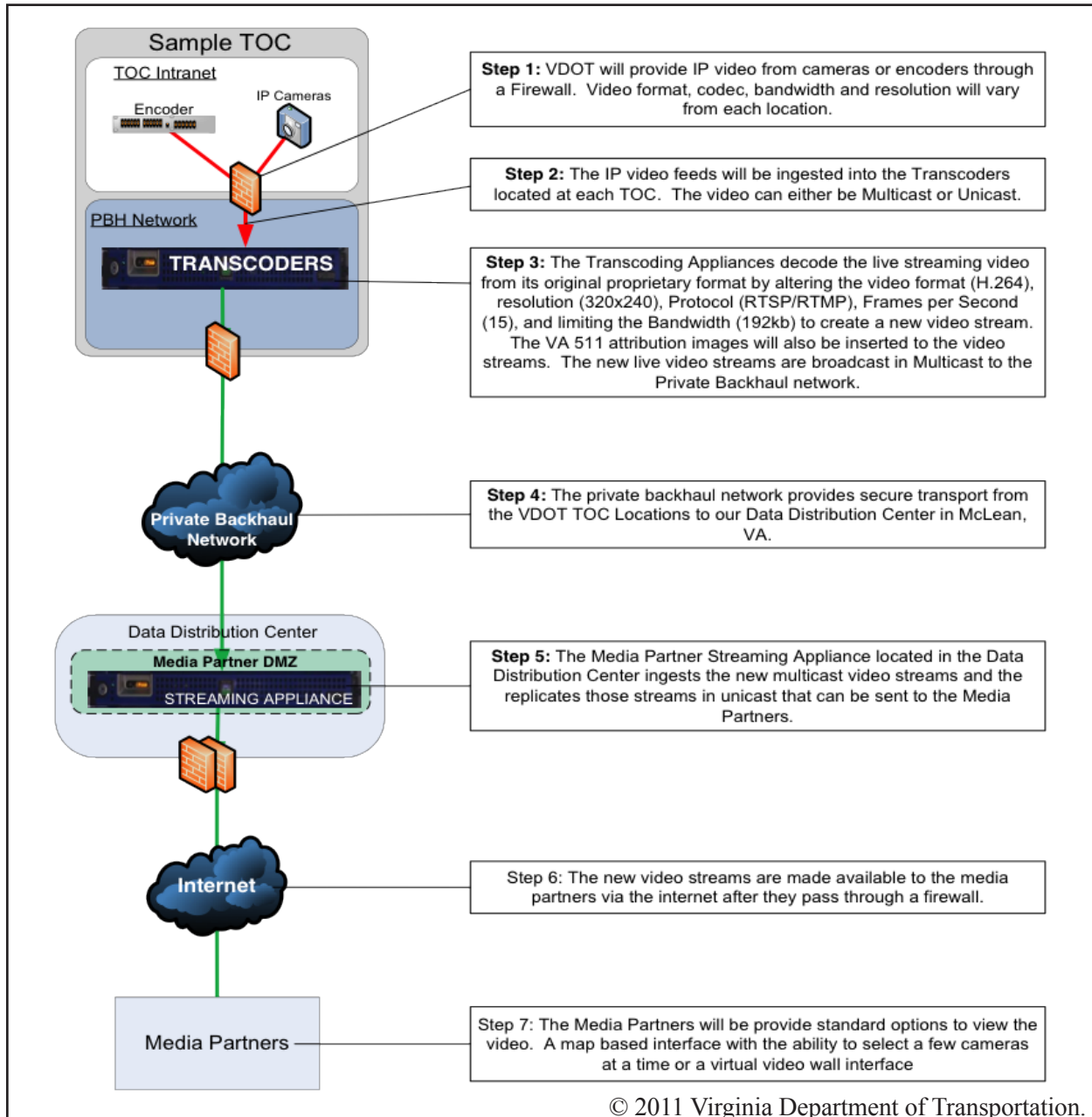
© 2019 North Carolina Department of Transportation.

**Figure 14. Illustration. Unique language from the North Carolina Department of Transportation media agreement requiring that the agency be given 15 public service announcement spots.**  
 Source: Agreement between NCDOT and media, North Carolina Department of Transportation. n.d. “Media Agreement.”  
 last accessed, May 1, 2019.

5 <https://www.cbs17.com/news/north-carolina-news/nc-bill-would-use-15m-to-help-record-ncdot-s-traffic-cameras/1818241319>.  
 6 <https://www.ncleg.gov/Sessions/2019/Bills/House/PDF/H227v0.pdf>.

## VIRGINIA DEPARTMENT OF TRANSPORTATION

In 2011, VDOT decided to outsource the serving of their video (and other data) assets through what they called their Traffic Video and Detection (TV&D) project. A core component of this program was to manage access to VDOT’s live video streams through a web portal found at: [https://www.vdotdatasharing.org/TVDDocs/Terms\\_of\\_Use.html](https://www.vdotdatasharing.org/TVDDocs/Terms_of_Use.html).



**Figure 15. Diagram. Virginia Department of Transportation video feed high-level network diagram.**

Source: Virginia Department of Transportation. n.d. “Feeds - Terms of Use” Web page.

Available at: [https://www.vdotdatasharing.org/TVDDocs/Standard\\_Video\\_Feed\\_Diagram.png](https://www.vdotdatasharing.org/TVDDocs/Standard_Video_Feed_Diagram.png),

last accessed May 1, 2019.



As part of this program, VDOT offers 15 frame per second video at 320 x 240 resolution at no cost to qualified users. However, the agency also offers 30 frame per second video at significantly higher resolution for media and other partners requiring this higher quality video. VDOT states that “All fees associated with the provision of high quality video are for cost recovery and will not contribute to revenue generation.”

**Table 6. VDOT Media Partner Video Transition Options**

	Standard Video Streams	Higher Quality Video Streams
Cost	Free	One time setup fee Monthly maintenance & Telco fees Optional custom interface
Video streams available	More than 75 publicly available VDOT supplied cameras	
Frames per second (FPS) bandwidth per stream resolution	15 FPS 192 kb per second 320 x 240	Up to 30 FPS 1000 kb per second Customized based on Customer Needs
Methods of access	All media members will be provided links (URLs) to the camera feeds	Media members will be provided a link to our video distribution network

Source: Virginia Department of Transportation. n.d. “VA511 Media Partner Video Transition Options.” Available at: [https://www.vdotdatasharing.org/TVDDocs/Video\\_Setup\\_Application\\_Handout.pdf](https://www.vdotdatasharing.org/TVDDocs/Video_Setup_Application_Handout.pdf), last accessed May 1, 2019.

Users interested in gaining access to the video feeds must first sign one of three different license agreements that are based on the expected use.

- Public entity for non-commercial use
- Private entity for non-commercial use
- Private entity for commercial use

One key stipulation of the video sharing agreement is that the VDOT logo must be displayed at all times over the video feeds—thus providing branding and attribution to VDOT. In principle, this makes sense—especially for broadcasters, as it provides marketing of VDOT services and traveler information to the broader public. In practice, however, the large branding banner and smaller logo can obscure critical information--especially when zoomed in to an incident scene.

## Licensing Issues

Proponents of VDOT’s TV&D licensing agreement report that it helps VDOT maintain stricter control over agency data assets, receive due credit for VDOTs information, and recoup the costs of the data feeds. Opponents of the agreement claim that they are overly restrictive, cause financial hardship to the public (but particularly the private) sector, and cannot be signed by some governmental agencies as a result of liability, indemnification, and other State-based laws. Certain clauses are deemed too risky or contrary to local laws to allow an agency to be able to sign the agreement and acquire access. Of the most concern is the clause that States begin “This Agreement and all amendments thereto shall be governed by the laws of the Commonwealth of Virginia...” Northern Virginia is part of the National Capital Region and borders Washington D.C. and the State of Maryland. For regional operations and coordination, it is imperative that State government agencies operating in these neighboring States be granted access to CCTV covering roads near borders. However, no State government will agree to abide by the laws of another State. This single clause has remained a frustrating barrier to CCTV sharing between government agencies.



**Figure 16. Photo. CCTV feed from the Virginia Department of Transportation 511 system.**

## APPENDIX A. EXAMPLE MEMORANDA OF UNDERSTANDING AND OTHER AGREEMENTS

### WEB-FORM FOR A LARGE, MULTI-STATE CCTV SHARING PROGRAM (SOME INFORMATION REDACTED).

Note that this is not a traditional MOU.

Participating Agency: \_\_\_\_\_

Requested by: \_\_\_\_\_ Date Requested: \_\_\_\_\_ Urgent:  Yes  No

Is this a temporary request?  Yes  No Date to be Removed by Participating Agency: \_\_\_\_\_

Reason for temporary request: \_\_\_\_\_

Name of User: \_\_\_\_\_ US Citizen:  Yes  No

Job Title/Job Function: \_\_\_\_\_

Email: \_\_\_\_\_ Phone: \_\_\_\_\_

MView Username is their email address (all lowercase)?  Yes  No

If not, please provide requested Username and reasoning for not conforming to the standard format:

\_\_\_\_\_

Level of access requested (to cameras/video from other Agencies)\*:  Level I  Level II  Level III  Level IV

\_\_\_\_\_

\* Upon approval and unless otherwise specified, the user would normally receive access the level requested as well as all levels below the requested level

Complete all that apply:

Criminal History Check completed with satisfactory results Date of Check: \_\_\_\_\_

Active Federal Security Clearance Date of Clearance: \_\_\_\_\_

Other (if selected, provide explanation below) Date, if applicable: \_\_\_\_\_

\_\_\_\_\_

#### Authorized Participating Agency Requestor Name and Contact Information:

Name: \_\_\_\_\_ Phone: \_\_\_\_\_ User Initials: \_\_\_\_\_

By submitting this request, the User and the Participating Agency have read and understand the Coordinated CCTV Concept of Operations (CCTV ConOPS). The User and Participating Agency agree to use the CCTV Sharing System, \_\_\_\_\_ or authorized business and in accordance with the CCTV ConOps.

PLEASE DO NOT WRITE BELOW THIS LINE

*This section is to be completed by \_\_\_\_\_ Administrator*

Access Granted:  Yes  No If applicable, state below why the request was not granted or only partially granted:

\_\_\_\_\_

Date Completed: \_\_\_\_\_ Administrator: \_\_\_\_\_

**TENNESSEE DEPARTMENT OF TRANSPORTATION**

**TRAFFIC OPERATIONS PROGRAM POLICY**

Effective Date:

**Title: Access to Live Video feeds and Information Sharing**

**POLICY**

The Tennessee Department of Transportation (TDOT) will make live video of traffic conditions from Closed Circuit Television (CCTV) available to the public. CCTV feeds from the Regional Transportation Management Centers (RTMC), located in Nashville, Knoxville, Chattanooga, and Memphis, will be supplied through TDOT’s SmartView CCTV web site. The video feeds provided are those made available by the RTMC Operators from the images on the traffic surveillance monitors within the RTMC and that are consistent with the objectives of traffic management.

Live video feeds will generally be made available upon request to other government and public agencies to better coordinate traffic management strategies on incidents and crashes, and to private news media and other organizations for their use in providing traffic information to the public or their customers.

A non-exclusive access Agreement is required in order for governmental and private interests to receive access to live video. Costs associated with the access connection, if any, will be determined by TDOT and may become the responsibility of the USER.

**BACKGROUND**

In order to gather realtime traffic condition information, TDOT has constructed and operates four Regional Transportation Management Centers located in Nashville, Knoxville, Chattanooga, and Memphis. The RTMC is the central collection point for roadway condition information. The RTMC support systems gather and disseminate traffic information using the latest technologies.

CCTV has proven to be a significant management and delay-reduction tool for the identification and verification of incidents and crashes, thereby enabling a proper and timely response. The sharing of video information enhances the communication of current traffic conditions, thereby aiding travelers in planning their trip times, routes, and travel mode using the latest available information. TDOT will operate and maintain the CCTV system for the purpose of enhancing traffic incident response on the Tennessee roadway system. TDOT wishes to share that traffic information with other transportation operating agencies, incident response agencies and the public.

**TENNESSEE DEPARTMENT OF TRANSPORTATION AND PRIVATE ENTITY USERS  
ACCESS AGREEMENT FOR LIVE VIDEO AND INFORMATION SHARING**

This Access Agreement for Live Video and Information Sharing is an Agreement between the Tennessee Department of Transportation (TDOT) and

\_\_\_\_\_ hereafter referred to as the “USER.” The effective date of this Agreement is \_\_\_\_\_.

The “Access to Live Video” is that video provided by a Closed Circuit Television (CCTV) system developed for traffic management and provided by the Tennessee Department of Transportation Regional Transportation Management Centers (RTMC) operated by TDOT. The CCTV feeds will show live traffic conditions including crashes, stalled vehicles, road hazards, weather conditions, traffic congestion, maintenance work, and repair work locations.

The purpose of providing the USER with Access to Live Video is to detect and disseminate realtime traffic information to motorists and improve incident response and recovery. The following provisions of this Agreement are intended to ensure that the CCTV system is accessed and its information is used for this purpose and this purpose alone.

Information Sharing, as defined in this agreement, is that information provided or discovered by the USER which has an adverse traffic impact on any Tennessee Interstate, State Route, and that which adversely affects travelers. Any information that falls within this definition will be shared with the TDOT RTMC within 10 minutes of receiving such information.

The USER hereby acknowledges and agrees that other matters not specifically addressed in this Agreement may arise and that TDOT shall have the right to make changes in this Agreement, by adding provisions, deleting provisions, and/or changing existing provisions when in TDOT’s opinion circumstances require such changes. TDOT shall provide prior written notice of any such changes to this Agreement to the USER at which time the USER may or may not accept the revisions. Not accepting future revisions may result in the USER being denied access to the live video feeds.

USER shall also retain the right to terminate this Agreement as provided herein.

**1. GENERAL INFORMATION:**

- A. TDOT will operate and maintain the CCTV system as a traffic management tool and, consistent with this purpose, TDOT agrees to provide the USER with Access to Live Video and Information Sharing. TDOT does not guarantee the continuity of this access, and TDOT does not warrant the quality of any video feeds or the accuracy of any image or information provided. Any reliance on such images or information is at the risk of the USER.
- B. TDOT will not record video feeds except for staff training purposes, and no recordings will be made available to the USER under this Agreement.

- C. TDOT will maintain exclusive control of the information and images released from the CCTV system to the USER, including but not limited to determining whether and when to provide a CCTV system feed, from what location, and for what duration. No feed will deploy the cameras' zoom capabilities, and no image will focus on vehicle license plates, drivers, or other personal identification of individuals involved in any traffic-related incident. No image will focus on any property or person outside the TDOT right-of-way. Access via feed will not be provided for events that are not, in the opinion of TDOT personnel, traffic-related. The decision whether to activate, and upon activation to terminate the access, is exclusively at the discretion of TDOT personnel.
- D. TDOT RTMC personnel will not accept requests that specific CCTV cameras are operated or repositioned.
- E. TDOT will provide each USER the same video feed from the CCTV system as any other USER participating in this Agreement. This Agreement in no way limits or restricts TDOT from providing video information to any other potential USER.
- F. TDOT reserves the right to terminate this video access program or to change the areas, times, or levels of access within the RTMC at any time.
- G. TDOT will provide Training Opportunities to all entities named in this Agreement and encourage participation in said training.

**2. USER'S RESPONSIBILITIES:**

- H. USER is exclusively responsible for any costs related to the purchase and installation of the equipment necessary to receive the live video feed. User will be required to remove previously installed equipment from the RTMC (if any). USER is exclusively responsible for any costs related to the removal of this equipment. USER must give RTMC personnel reasonable advance notice to schedule an appointment to remove equipment and RTMC personnel reserve the right to schedule such at a time and in such a manner so as to not interrupt or otherwise obstruct RTMC operations. USER staff at the RTMC shall be under the general direction of the RTMC Manager for routine conduct, privileges, and protocols within the RTMC.
- I. USER shall maintain the security and integrity of the CCTV system by limiting use of the system to trained and authorized individuals within their organization, and by insuring the system is used for the specific purpose stated in this Agreement. No feed shall be purposely broadcast live or rebroadcast that is zoomed in on an incident where individuals or license numbers are recognizable.
- J. USER accepts all risks inherent with the live video feeds, including, but not limited to, interruptions in the video feed, downtime for maintenance, or unannounced adjustments to the camera displays. TDOT is providing the video feeds as a convenience to the USER and agrees to provide a good faith effort to maintain the video feed from TDOT equipment. The USER agrees to hold TDOT harmless, including TDOT employees and TDOT designated agents, from any damages caused to USER by loss of a video signal due to equipment failure or any act or omission on their part.

- K. USER agrees to provide TDOT with a technical contact person and with a list of all USER personnel trained to operate the TDOT SmartView system. USER shall limit technical calls to the RTMC for monitoring, diagnosing problems or otherwise performing any minor service on the SmartView system.
- L. USER agrees to acknowledge that the video feeds are provided by the Tennessee Department of Transportation.
- M. USER agrees to display the SMARTWAY logo in the upper left hand corner of any view provided outside of the agency.
- N. USER agrees to provide timely, accurate information and assistance to TDOT or other agencies, responders and roadway users about roadway conditions, major and minor incidents and alternate routes through the use of any media and USER resources.
  - i. USER agrees to notify the RTMC of their surrounding TDOT Region of any unexpected incidents that are expected to have an adverse impact on traffic operations of Interstate or State Routes, within 10 minutes of first notification to the USER. This applies to any incident where TDOT or the Tennessee Highway Patrol is not already on-scene. Unexpected incidents may include, but are not limited to: traffic crashes, disabled vehicles, roadway debris, hazardous weather conditions, traffic queues, or traffic signal failures.
  - ii. USER agrees to collaborate with TDOT with respect to traffic management of planned events that are expected to have an adverse impact on traffic operations of Interstate or State Routes. Planned events include temporary traffic generating events (such as concerts or fairs) and roadway work zone activities (such as construction or maintenance activities). Collaboration and information sharing between USER and TDOT should occur as early as possible.
- O. USER is invited to participate in quarterly Regional Traffic Incident Management meetings and may attend any traffic incident management training provided by participating agencies.

**3. LIABILITY AND INDEMNITY PROVISIONS:**

- P. USER agrees to defend, indemnify, and hold TDOT harmless from and against any and all liability and expense, including defense costs and legal fees, caused by any negligent or wrongful act or omission of the USER, or its agents, officers, and employees, in the use, possession, or dissemination of information made available from the CCTV system to the extent that such expenses or liability may be incurred by TDOT, including but not limited to, personal injury, bodily injury, death, property damage, and/or injury to privacy or reputation.
- Q. The liability obligations assumed by the USER pursuant to this Agreement shall survive the termination of the Agreement, as to any and all claims including without limitation liability for any damages to TDOT property or for injury, death, property damage, or injury to personal reputation or privacy occurring as a proximate result of information made available from the CCTV system.

**4. TERMINATION:**

R. TDOT or USER may terminate this Agreement at any time for any reason by providing written notice of termination.

**State of Tennessee Department of Transportation**

Approved as to Form:

By: \_\_\_\_\_  
John Schroer  
Commissioner

\_\_\_\_\_  
John Reinbold  
General Counsel

Date: \_\_\_\_\_

USER AGENCY \_\_\_\_\_

By \_\_\_\_\_

(Print Name) \_\_\_\_\_

(Title) \_\_\_\_\_

Date: \_\_\_\_\_

Approved by Legal Counsel for USER AGENCY

By \_\_\_\_\_

(Print Name) \_\_\_\_\_

(Title) \_\_\_\_\_

Date: \_\_\_\_\_



## MAJOR MULTI-STATE VIDEO SHARING CONOPS DOCUMENT (NO MOU USED)

### Coordinated CCTV Concept of Operations Key Points

By developing specific guidelines and policies for video data exchange, government and approved private entities operating will have a formal process to facilitate timely exchange of information related to Closed Circuit Television (CCTV). Policies will be in place governing usage and restrictions on use and the agreed-upon parameters will ensure that the data being exchanged is of a standard format, quality and detail level. (Section A - Introduction)

*All live video images obtained from the Originating Agency's Video/Imaging Systems are the exclusive property of the Originating Agency and may be used only with permission of the Originating Agency or their designee by granting access in the CCTV Sharing System. (D.1 – Confidentiality and Ownership)*

All live video images remain under the control of the Originating Agency, both for sharing with other agencies, the public, or in response to disclosure requests under public information laws or discovery requests. (D.3 – Confidentiality and Ownership)

All technical information regarding video surveillance systems, including connectivity and transmission information, the operational readiness of imaging systems, access control systems, and security response plans or procedures is confidential and restricted and may not be disclosed, viewed, reviewed, or transmitted by any means to unauthorized users. (D.2 – Confidentiality and Ownership)

There are four access levels of sharing live video images, Level 1 being the least restrictive and Level 4 the most restrictive. The Originating Agency has the responsibility to set levels for their cameras and can change them at any time, with notice to MCAC and other relevant agencies. The Originating Agency may further restrict access at its discretion. It is the responsibility of each Agency to request particular access levels for its employees or contractors (to cameras/video from other Originating Agencies) and provide necessary documentation, such as security clearance information. (Section E – System Access Authorization)

In order to obtain access to the CCTV Sharing System, each applicant requires a documented need to access the system based upon the duties and responsibilities of his or her employment. This need must be verified by the head of the applicant's agency or organization, or by his or her designee. (Section E – Access Requirements)

It is recommended that each Agency use the -UserAccess-RequestForm referenced in Appendix B to make such requests. (Section E – System Access Authorization) The form may be used by a Participating or Originating Agency's CCTV Administrator or its designee in requesting CCTV access to cameras/video from other Originating Agencies for their employees and contractors in the CCTV Sharing System. (Appendix B.1.a --UserAccess-RequestForm)

*Note: The form designates a request for level of access to cameras/video from other Originating Agencies.*

The Originating Agency will maintain pan/tilt/zoom (PTZ) control of their video system’s cameras. Camera PTZ control will reside with the Originating Agency’s operational group having overall monitoring responsibility. A Participating Agency can request PTZ adjustments of the Originating Agency for a particular video. The Originating Agency has full discretion to approve or deny requests for PTZ changes or control by a Participating Agency on a case by case basis. (Section G – Camera Pan/Tilt/Zoom Control)

*Note: If an Originating Agency temporarily blocks a particular live video image from their system for maintenance, technical difficulty, etc., an user will lose the ability to view that live video image during that time.*

The Originating Agency’s Video/Imaging Systems and any associated live video images, information, and the archives produced from these systems are government resources and the exclusive property of the Originating Agency. These government resources are provided to enhance a Participating Agency’s authorized users’ ability to maintain a safe and secure environment for their agency’s employees and contractors, its customers, and its property or to meet their agency mission. Any other use of the Originating Agency’s Video/Imaging Systems and associated live video images, information, and archives is prohibited and a violation of this policy. (Section F.1 – System Inappropriate Use)

Access to recorded video shall be by written request to the Originating Agency, or by written agreement of the requesting agency and Originating Agency, or by request to MCAC who would forward the written request to the appropriate Originating Agency. The CCTV Video Access Request Form may be used to request recorded video from an Originating Agency and may also be used internally within an Originating Agency. (Appendix B.1.b – CCTV-VideoAccess-RequestForm)

All authorized users must be individually identified with unique login credentials within the CCTV Sharing System. The use of their login credentials is acceptance of the terms of this agreement. (Section F.2 – System Inappropriate Use)

Any employee or contractor of a Participating Agency violating this policy is subject to disciplinary action by the Participating Agency and to applicable federal, state, and local laws. (Section F.3 – System Inappropriate Use)

## **VIRGINIA DEPARTMENT OF TRANSPORTATION TERMS OF USE**

Virginia Department Of Transportation MOUs for Public and Private Entities can all be found at [https://www.vdotdatasharing.org/TVDDocs/Terms\\_of\\_Use.html](https://www.vdotdatasharing.org/TVDDocs/Terms_of_Use.html) and their CCTV attribution guide can be found here: [https://www.vdotdatasharing.org/TVDDocs/VDOT\\_CCTV\\_and\\_Data\\_Attribution\\_Guide\\_-\\_v6.pdf](https://www.vdotdatasharing.org/TVDDocs/VDOT_CCTV_and_Data_Attribution_Guide_-_v6.pdf).



## APPENDIX B. VIDEO SHARING PRACTICES

Minnesota Department of Transportation Questionnaire for Vendors (filled out by Skyline Technology Solutions)

### Streaming Video Sharing Practices

Questionnaire Guide: Vendors  
May 2, 2018



#### TECHNICAL DETAILS AND SPECIFICATIONS

1. What hardware (e.g. encoders, servers) is supported, including specifications, to deliver streaming video service?
  - a. Skyline supports all IP video streams that originate from cameras, encoders or video management devices. These include:
    - i. VMS - Milestone, Genetec, Cisco, Onssi, and many others to source the video streams.
    - ii. Camera Encoders – Cohu, WTI, Axis, Sequira/Optelecom, Cortec, Bosch, Pelco, and many others.
  - b. Skyline’s ability to normalize any IP video stream to a standard H.264, RTP, frame rate, bandwidth, and resolution allows Skyline to ingest any legacy IP video stream. We have created a transcoding hardware appliance to handle this process for all legacy video feeds. Modern cameras can provide a native standard stream.
  
2. What format is video delivered in and is it selectable?
  - a. RTSP – for Video walls, VMS, and any solution using a VLC player.
  - b. RTMP/Flash – web enabled portals, browsers are starting to phase this out.
  - c. CLSP – created by skyline to replace the low latency, highly scalable RTMP (HTML5 Compliant).
  - d. HLS/HTTPLive – used by all Mobile phones and tablets (HTML5 Compliant).
  - e. The video is delivered in the format required by the end device of the user requesting the video without any intervention from the user.
  
3. How much bandwidth is needed and how is it balanced for daily non-peak, peak, and big surges related to weather events or major incidents?
  - a. Public and large scale partner distribution is generally distributed at 192kb per stream 15 frames per second, 320x240 resolution.
  - b. Our solution requires one stream from each video source. If the video requires normalization, it is first pulled into our transcoding appliance. From there, the video is sent to our streaming appliances, which are either located on the client’s ISP, or in many cases the streams are sent to our data center.
  - c. The streaming appliances can handle 400 unique source feeds and can provide up to 4,500 views from each appliance based on 192kb feeds. During times of peak demand, your internal network will only pull one stream from the camera. The streaming appliance provides the replication point.

- d. 1,000 feeds would require 3 streaming appliances and could support 13,500 concurrent feeds, if request exceed that amount another steamer could be added to distribute the load.
  - e. Our large hosted clients share a 1gbps ISP that can burst up to 10gbps if required.
  - f. Winter storms over the last several years demonstrate large amounts of viewers over 12- 16 hours with no issues.
  - g. An additional higher bandwidth stream can be pulled from the camera for use in the TMC and potentially sent to the media. This is up to the source agency and these feeds are general set up as on-demand. Meaning the video stream is only requested from the internal network upon request. This reduces the impact of large resolution video.
4. Who provides bandwidth – the agency, an enterprise agency, or the vendor?
    - a. Client’s choice – it depends upon the capacity of their own ISP services and infrastructure.
      - i. Manage their own ISP - Maryland, Pennsylvania, Missouri, West Virginia.
      - ii. Skyline hosts ISP – Virginia, South Carolina, Michigan, Tennessee, DC, (soon Texas and NYS).
  5. Similar to bandwidth management, how is load balancing managed on the server side?
    - a. Skyline scales the appliances based on the expected highest load, we typically include a spare appliance at each location to facilitate immediate replacement to avoid any breaks in service. We can also monitor usage of particular cameras. If a particular camera is seeing consistently excessive use, then we can simply move cameras around to other streaming appliances to accommodate.
    - b. Because you have the ability to track the usage overtime you can then make architectural changes.
  6. What type of firewall equipment is used to ensure security yet facilitate access?
    - a. Depending on the client Skyline can provide a firewall or can work with the client to configure their firewall.
    - b. Skyline is a network engineering company by birth, we manage statewide networks and are familiar with all manufactures and types of firewalls.
    - c. Our solution is designed to align with agency security rules. All video is provided from a network DMZ that is managed by the firewall. Users make requests for video only over ports 1935 and 554 and will only ever be able to access the streaming appliance on the DMZ. Separating the internal from the external.
  7. How can software requirements or plug-ins (e.g. Flash) that are likely to interfere with user security restrictions be avoided? Are solutions such as HTML5 being implemented or considered?
    - a. Currently our solution provides RTSP, RTMP, CLSP and HLS today.
    - b. Both HLS and CLSP are HTML5 compliant.
    - c. When a site uses a player it can dictate the format requested.

8. Does MnDOT’s process of re-encoding video from multiple cameras and formats to provide a consistent overall video format for a feed save any costs?
  - a. Yes. If you are able to provide all your video feeds in H.264, RTSP, and the correct frame rate and size, that will avoid the need to install any Transcoding/Normalizing appliances.
9. What platforms can video be delivered to – desktop, mobile, etc.?.
  - a. Any device that can play h.264 video, the solution is designed to support any player on any device.
10. How is video labeled to identify date, time, location, etc.?.
  - a. Placing external embedded images can be done during normalize process, this is very processor intensive and would require a large amount of hardware.
  - b. We suggest providing this information in the video player as a label or title for the video.
  - c. Another option is to apply a label at the camera itself.

### USER GROUP MANAGEMENT

11. Can different qualities of video be provided to different user groups? For example, higher quality for broadcast media and lower quality for the public.
  - a. Yes, with an additional higher quality feed pulled from the camera, Skyline can provide high and low quality feeds to separate user groups.
  - b. We would set up separate streamers to pull in the higher quality streams. Which allows the agency to use an access list on their firewall to limit access to the high quality streaming appliance.
12. How is blocking sensitive video managed across different groups of users?
  - a. Skyline has a stream manager that allows the client to block any feed to any group of users. When public and media are cut off, the trusted partners can still see the video streams.
  - b. Skyline has also used API’s to integrate with ATMS applications so operators can check a box in the application that sends an offline message to the stream manager.
13. What options are available to support multi-agency (e.g. police, cities, counties) sharing – in terms of both technical and cost-sharing features?
  - a. Skyline has created several portals to support multi-agency video sharing.
  - b. The Claris portal provides interface and access management to trusted partners. Typically, the DOT purchases this software and then provides access to the portal for its partners.
  - c. Cost savings comes from not maintaining one off connections or user licenses for other applications.
14. Can video from other agencies be streamed through the same system that distributes it?
  - a. Yes, in most states the DOT will incorporate video from counties, cities, and other public agencies.

- b. The other source agencies can also provide their own video.
  - c. Skyline can provide any support needed to incorporate those video sources.
- 15. Are users given multiple video feeds (e.g. video from several cameras in one browser window) or are they restricted to one feed (e.g. video from one camera in a browser window)?
  - a. Claris portal can display as many cameras as the pc can handle.
  - b. Most 511 sites restrict the viewer to one camera.
  - c. Other portals can play as many as the would like.
- 16. Is video provided as a continuous feed, if requested, or are time outs built into the feed?
  - a. Videos are continuous.
  - b. Timeouts are typically done at the application level.
- 17. Is there a “dispatch center” option that allows multiple cameras to be opened in a window, without timing out?
  - a. Claris can be configured to stay on continuously, this is done specifically for operation centers.
- 18. How are user accounts managed (e.g. adding accounts, resetting passwords) and what lessons can be shared?
  - a. Claris has a robust multi-level admin approach. Each agency maintains their users, cameras, device groups and most importantly who has access to their cameras.
  - b. Other agencies maintain who can access their cameras, and so on.
  - c. Our clients have SOP’s, agreements and service level expectations that can be repurposed by new clients to support their video sharing programs.

### **EXPERIENCES WITH DOTS**

- 19. How is streaming video integrated with existing traveler information services?
  - a. Skyline provides API’s to all the 511 applications from our Stream Manager which also provides the meta data for the cameras. Typically the sites poll the API to get updates status’ on the cameras.
- 20. Can vendors describe cost and technical incentives along with case studies?
  - a. Yes, we can supply case studies and will forward to you separately upon request.
  - b. Skyline will provide a high level ROM no later 6/15/18. Each state has many variables that impact the amount and location of equipment which impacts cost. So we can provide a more specific ROM for MnDOT.
- 21. Are advertising or other mechanisms ever used to offset costs?
  - a. This has been tried many times and not much revenue has ever been provided. Challenges are speed of decision making, many browsers already saturate the market with cookie related marketing.



22. What have your experiences been with providing this kind of services for DOTs?  
Any lessons learned that could improve the process?
- a. We currently support video distribution in 8 states and DC, and are in the process of adding NY and TX.
  - b. We provide 24/7 support and for hosted clients we monitor the appliances and network via our 24/7 Network Operations Center located at our office with a redundant site at one of our three supported data centers. This means you call skyline and receive a ticket for every issue you report or that we find through monitoring.
  - c. Utilization is highest during the late afternoon.
  - d. Skyline understands your network environment and will always consider all network implications when implementing appliances in your environment. Moving video around tends to shed light on network vulnerabilities and we are well versed in identifying and recommending solutions for those.





Federal Highway Administration  
U.S. Department of Transportation  
1200 New Jersey Avenue, SE  
Washington, DC 20590  
<https://ops.fhwa.dot.gov>

September 2019

FHWA-HOP-19-037



U.S. Department of Transportation  
**Federal Highway Administration**