Transportation Management Center Video Recording and Archiving Best General Practices

March 2016

U.S. Department of Transportation
Federal Highway Administration

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.

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. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-HOP-16-033		

4. Title and Subtitle	5. Report Date
Transportation Management Center Video Recording and Archiving Best General Practices	March 2016
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Stephen Kuciemba, Kathleen Swindler	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
WSP | Parsons Brinckerhoff Under contract to: Cambridge Systematics, Inc. 4800 Hampden Lane, Suite 800 Bethesda, MD 20814	11. Contract or Grant No. DTFH61-12-D-00048 T-5009

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Highway Administration 1200 New Jersey Avenue, SE Washington, DC 20590	Final Report, March 2015 to March 2016
	14. Sponsoring Agency Code HOP

15. Supplementary Notes

Government Task Manager: Jimmy Chu

16. Abstract

Closed-circuit television (CCTV) cameras are an important tool for transportation agencies who rely on them for incident verification, response preparation, traffic management awareness, special events, weather conditions, and much more. In some instances, these agencies have considered recording all or some of the video feeds—and in many instances agencies are sharing video with other transportation and law enforcement agencies.

This report presents a cross section of how different agencies are addressing video recording and sharing topics—drawn from a literature review, online inquiry, interviews, and expert input. Since State and local regulatory, policy, operational, and fiscal environments differ (in some cases quite significantly) it is a challenge to identify one-size-fits-all best practices. Therefore this report presents best general practices for Transportation Management Center (TMC) leaders to consider and in some instances recognizes that several different practices might apply (specific to the needs of an agency or organization).

17. Key Words	18. Distribution Statement
Closed-circuit television (CCTV) cameras, Transportation Management Center (TMC), video, incident verification, response preparation, best practices	No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	118	N/A

EXECUTIVE SUMMARY

Closed-circuit television (CCTV) cameras are an important tool for transportation agencies who rely on them for incident verification, response preparation, traffic management awareness, special events, weather conditions, and much more. In some instances, these agencies have considered recording all or some of the video feeds—and in many instances agencies are sharing video with other transportation and law enforcement agencies.

This report presents a cross section of how different agencies are addressing video recording and sharing topics—drawn from a literature review, online inquiry, interviews, and expert input. Since State and local regulatory, policy, operational, and fiscal environments differ (in some cases quite significantly) it is a challenge to identify one-size-fits-all best practices. Therefore this report presents best *general* practices for Transportation Management Center (TMC) leaders to consider and in some instances recognizes that several different practices might apply (specific to the needs of an agency or organization).

TMC managers report that they can be successful under any of the three fundamental video recording approaches—always (continuously record most feeds), sometimes (initiate recording of individual feeds for specific events), and never. There are benefits and limitations to each approach, often specific to the current environment within the agency, and this report attempts to portray the many different scenarios that may be present.

The best general practices cover a wide range of issues, including:

- **Technical—**Example: consider a software feature that enables automatic screen shots of a composite of selected camera feeds—useful for incident clearance performance management.
- **Operational—**Example: when saving video clips, use a consistent and searchable file name structure, and keep the request process simple and scalable. Consider using forms linked to tracking databases to reduce manual data entry.
- **Policy—**Example: to support Transportation Systems Management and Operations (TSMO) collaboration with local agencies, use recent, local clips in Traffic Incident Management (TIM) training. Also consider including TIM participation as a precondition of sharing streaming or recorded video.
- **Legal—**Example: since State Freedom of Information Act (FOIA) and record retention laws differ, ask Counsel if your State's FOIA equivalent law has language on video recordings and differentiates between "raw data" and "records."

The best general practices are based primarily on the experiences of agencies. This report presents findings in chapters that include recording and using video, fulfilling requests for recorded video, sharing real-time images, legal and policy issues including the Freedom of Information Act (FOIA), and written policies. It also highlights seven case studies from transportation agencies that bring attention to differences in their policies and practices in an instructive manner.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

AIRS	Auto Incident Record System
ASF	Advanced Systems Format
ATMS	Active Traffic Management System
BVMS	Bosch Video Management System
CARS	Condition Acquisition and Reporting System
CCTV	Closed-circuit television
DOT	Department of Transportation
DVR	Digital Video Recorder
FAQ	Frequently Asked Questions
FDOT	Florida Department of Transportation
FOIA	Freedom of Information Act
fps	Frames per second
FTE	Full-Time Equivalents
FTP	File Transfer Protocol
HOT	High-Occupancy Toll
HOV	High-Occupancy Vehicle
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transportation Systems
MSA	Metropolitan Statistical Area
MnDOT	Minnesota Department of Transportation
MOU	Memorandum of Understanding
MSP	Minnesota State Patrol
NITTEC	Niagara International Transportation Technology Coalition
NJDOT	New Jersey Department of Transportation
NMDOT	New Mexico Department of Transportation
NTCIP	National Transportaion Commission for ITS Protocols
NVR	Networked Video Recorder
NYSDOT	New York State Department of Transportation
ODOT	Oregon Department of Transportation
RTC	Regional Transportation Commission
RTMC	Regional Transportation Management Center
SA	Self-Assessment
SPCA	Society for the Prevention of Cruelty to Animals
STMC	Statewide Traffic Management Center
STOC	Statewide Traffic Operations Center
TDOT	Tennessee Department of Transportation
TIM	Traffic Incident Management
TMC	Transportation Management Center
TRIMARC	Traffic Response and Incident Management Assisting the River Cities
TSMO	Transportation Systems Management and Operations
VHS	Video Home System
WisDOT	Wisconsin Department of Transportation
WSDOT	Washington State Department of Transportation

CHAPTER 1: INTRODUCTION AND REPORT LAYOUT

BACKGROUND

Today's Transportation Management Center (TMC) has become a clearinghouse for closed-circuit television (CCTV) images, with traffic cameras owned by many different agencies often streaming images through this focal point of activity. TMCs may handle hundreds of cameras and share feeds not only with peer transportation management agencies, but with law enforcement, with emergency response agencies, and with the public. Policy decisions can have major impacts on the effectiveness of CCTV as a management tool. Procedures and technologies can also have major impacts on staffing needs and operational costs. Recognizing the importance of these topics, the members of the TMC Pooled Fund Study (PFS) prioritized this project. While the legal and resource frameworks vary among agencies, the objective of this task report is to help TMC operators by identifying best general practices for TMC video camera recording and archiving, as well as video sharing and legal issues. This report captures the important findings for use by PFS members and other interested parties.

REPORT OBJECTIVES

The core report objective is to provide information on best general practices in TMC video recording, archiving, and sharing that will help TMC operators make informed decisions on practices within their own unique set of policy, operational, and technological constraints. To support this core objective, the report synthesizes information from available literature with the experience from TMC operators, PFS members, equipment vendors, and consultant team experts. It presents a sampling of TMC video policies and procedures from around the country, provides case studies with more detail, presents legal and technical reference information, and includes copies of select written policies. Drawing from all of this material, the report also includes best general practices to highlight questions and actions for agencies to consider for their operations.

This report does not cover video used for toll processing, for automated enforcement (e.g., red light running or speed enforcement), or for security-focused functions. While those types of video cameras may sometimes be co-located with TMC functions, they are significantly different from traffic management and are outside the scope of the project.

SOURCES

Information contained within this report is drawn from a review of published literature, an online inquiry to selected TMC representatives, review of documents provided by agencies, interviews with TMC PFS members/TMC operators, and insight from the consulting team's experts.

The list of the 52 Metropolitan Statistical Areas (MSA) with populations over one million was used as a starting point to identify a representative sample of individuals and TMCs. Note that some MSAs are served by multiple TMCs and some TMCs service multiple MSAs.

Representatives of the identified TMCs were invited to participate in an online inquiry that was structured as a quick, user-friendly way for them to provide input on their own schedules. A total of 26 individuals responded to the request for information covering a total of 32 of the originally targeted TMCs. See table 1 for a list of represented agencies.

Table 1: Responding agencies to online inquiry.

California DOT (Caltrans)	Minnesota DOT	Tennessee DOT
Florida DOT	New York State DOT	Texas DOT
Illinois DOT	Niagara International Transportation Technology Coalition	Virginia DOT
Iowa DOT	North Carolina DOT	Washington State DOT
Maryland State Highway Administration	Ohio DOT	Wisconsin DOT
Massachusetts DOT	Regional Transportation Commission of Southern Nevada	
Michigan DOT	Road Commission for Oakland County (Michigan)	

Note: In some cases, participants indicated that their responses applied to multiple Transportation Management Centers within the target list. Department of Transportation is abbreviated as DOT.

In support of the initial online inquiry, more extensive phone interviews were conducted with representatives from more than a half dozen agencies to discuss their practices, experiences, and decisionmaking processes in further detail. The results are interspersed within this report and also form the basis of chapter 8, Case Studies. The agencies from which representatives were interviewed are the Iowa, Minnesota, New Jersey, Tennessee, Washington, and Wisconsin Departments of Transportation, and the Regional Transportation Commission of Southern Nevada. They were selected as a sample to cover a range of approaches to different fundamental policy choices, to represent a variety of geographical perspectives, and in some instances to highlight agencies that have recently changed policies.

REPORT ORGANIZATION

The topics of video recording and video sharing are comprised of many interconnected and overlapping issues. This report addresses each of the major recording policy options, including from the legal/policy, operations, and technology perspectives. Although the issues are interrelated, the chapter organization below was developed to provide a logical structure for presenting the information. A brief description of each chapter is as follows:

- **Chapter 1: Introduction and Report Layout.** An overview of the report's objectives, sources, and organization intended to provide sufficient background for the reader not previously familiar with the project.
- **Chapter 2: Successful Practices for Recording and Using Video.** This chapter includes a brief discussion of the basic policy question—whether to record always, sometimes, or never. It covers some of the decision factors present in different operating environments. This chapter also covers topics specific to recording and using video, including the use of capability maturity models (CMM) to assign a measure to an organization's procedures and strategy.
- **Chapter 3: Successful Practices for Fulfilling Requests for Recorded Video.** A detailed discussion of the various processes used by TMCs to respond to requests for recorded video from the public and from other agencies.
- **Chapter 4: Successful Practices for Sharing Real-Time Video Images.** How some agencies mitigate the risks and deal with the constraints associated with sharing real-time video images with other agencies and with the public.
- **Chapter 5: Technology Issues.** This chapter includes an overview of camera and recording technology topics, plus a checklist of considerations for recording systems.
- **Chapter 6: Legal and Policy Issues including the Freedom of Information Act (FOIA).** Since the legal issues vary by State, this chapter identifies issues, provides general information, and gives recommendations on how agencies can seek the knowledge they need to make informed decisions on portions of policy and procedure that are within their control.
- **Chapter 7: Practices for Written Policies and Agreements.** Institutions often have varying perspectives on the need for various types of written policies. This chapter presents some of the successful practices for consideration.
- **Chapter 8: Case Studies.** The case studies in this chapter show a range of policy and procedure approaches that TMCs are using to maximize the potential benefits of recording and sharing video within their individual policy, institutional, technological, and fiscal constraints.

Best general practices are highlighted by showing them in call-out boxes throughout chapters 2 through 7. The best general practices are derived primarily from the experiences of agencies, and in many cases were drawn directly from the case studies. By embedding them in the chapters, however, they retain their context and provide more direct benefit for the reader who may only be interested in one or two of the issue areas.

CHAPTER 2: SUCCESSFUL PRACTICES FOR RECORDING AND USING VIDEO

Closed-circuit television (CCTV) cameras are an important tool in the transportation management toolbox. Transportation agencies rely on them for incident verification, response preparation, traffic management awareness, special events, weather conditions, and much more.

The operational benefits of real-time video are somewhat obvious—so why would an agency also be interested in recording or archiving any of this CCTV video footage?

Once an agency has wrestled with the question of WHY they should record, it next comes down to whether or not they WILL record. This chapter draws upon the opportunities (purposes of recorded video) and constraints (records retention, costs, technology, liability, and privacy) to discuss how agencies make the major decision. This chapter describes the major policy decision in terms of three simplified terms for possible policy options: ALWAYS, SOMETIMES, and NEVER.

Chapter 2 is the first in a series of chapters that provide more detail on groups of issues within the major policy choices of when to record video. The information is meant both to improve the practices of agencies committed to certain policy choices and to provide background to agencies that may be reconsidering their current policy choices. This chapter is also the first to give insight into the relative prevalence of various policies and practices by presenting graphics of results from the online inquiry sent to Transportation Management Center (TMC) staff from around the country.

USES AND BENEFITS OF RECORDED VIDEO BY ROADWAY AGENCIES

Recording and archiving traffic video offers a number of benefits to agencies. As shown in figure 1, TMCs are interested in having recorded video for a variety of purposes with training being the most common.

Some of the types of data collected included bicycle counts, pedestrian counts/flows, vehicle counts for signal timing, observation of merging zones, and observation of a roundabout to be used addressing crash issues.

The “other” category included a variety of responses including allowing media to record brief clips for reporting, capturing transition of reversible lanes, and after-action reviews (which one could argue may be defined the same as training or incidents in the eyes of some respondents). New Jersey’s Statewide Traffic Management Center (STMC) noted that it is using temporary cameras in work zones to record intermittent screen shots to create time-lapse films of construction progress and to be able to verify actual timing of lane closures.

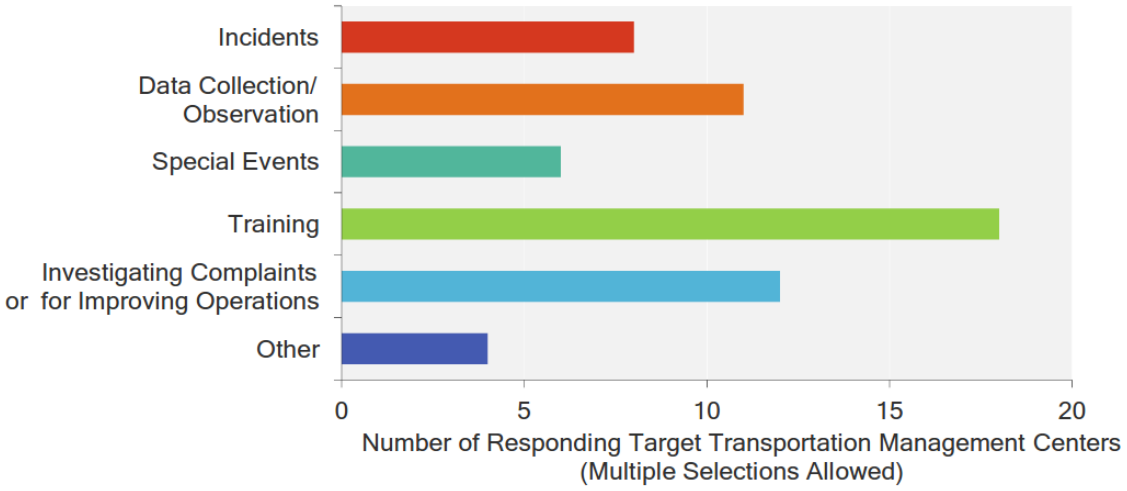


Figure 1: Chart. Purposes of selective video recordings.
(Source: Parsons Brinckerhoff.)

The Wisconsin Department of Transportation (WisDOT), which records most feeds most of the time, summarized the benefits of recording video in their 2013 webinar "CCTV Role in WisDOT's TIM [Traffic Incident Management] Success":

- The Department of Transportation (DOT) and emergency responders reviewed incidents for lessons learned, best practices, incident debriefs, and emergency traffic control and scene management guidelines.
  - Traffic Incident Management (TIM) education and training.
  - Improved TIM increases safety and provides economic benefits (travel-time savings).
- Unintentional benefits to law enforcement, both for recording crimes and for enabling investigators to place vehicles or suspects at a specific time and location.

Agencies agreed that the primary purpose of traffic camera video, whether recorded or not, was for traffic management. Additional benefits may exist, such as recordings for evidence of crimes, but TMCs should be clear that their systems were not designed for or intended to be security systems.

Many of the benefits of recorded/archived video are still relatively new to agencies that have only recently upgraded some of their technology and operating systems. Improved digital video recorders and storage units have opened the door to a number of new opportunities and the realization of benefits may be new. A more detailed discussion on technology improvements is featured in chapter 5.

Best General Practice

Be clear that the primary purpose of traffic video is for traffic management, not security, noting that the traffic systems were not designed or intended to meet security system requirements.

FUNDAMENTAL RECORDING POLICY QUESTION—ALWAYS, SOMETIMES, OR NEVER

For the purposes of this report it was important to develop general categories to organize the major recording issues. Three groupings of possible policy options are presented as simplified one-word terms: Always, Sometimes, and Never.

- **ALWAYS**—A generalized short-hand for the policy of automatically recording all feeds continuously. Agencies in this category report that in reality this becomes most of the feeds most of the time, recognizing that it is not feasible to record every feed 100 percent of the time due to equipment failures, system maintenance, and special exceptions. This category refers to automatic recording by default. While many feeds are continually recorded, they may only be retained for a few days unless an action is taken by a staff member to save a particular clip longer.
- **SOMETIMES**—A generalized short-hand for the policy to only record select feeds for specific purposes. By default, feeds are not recorded. An action must be taken by an operator to initiate recording, typically for a limited amount of time to capture an event or period of data collection. This category refers to selective recording or recording only under limited circumstances.
- **NEVER**—A generalized short-hand for the policy of not recording full-motion video at all, though in practice there may be static image capture or very rare occasions where some clips are retained.

Note that in this chapter the term "record" refers to any retention of video regardless of duration. It is important to note, however, that some agencies differentiate between "record" and "archive" as follows:

- Record—denotes video retained only until it is automatically overwritten.
- Archive—when video clips have been selected for retention beyond the automatic overwriting.

Figure 2 shows that amongst the agencies contacted, only a few chose not to record video—the NEVER category. At the opposite end of the spectrum, only a few agencies recorded most of the time—the ALWAYS category. The most common general practice is to record under limited circumstances for specific purposes—the SOMETIMES category.

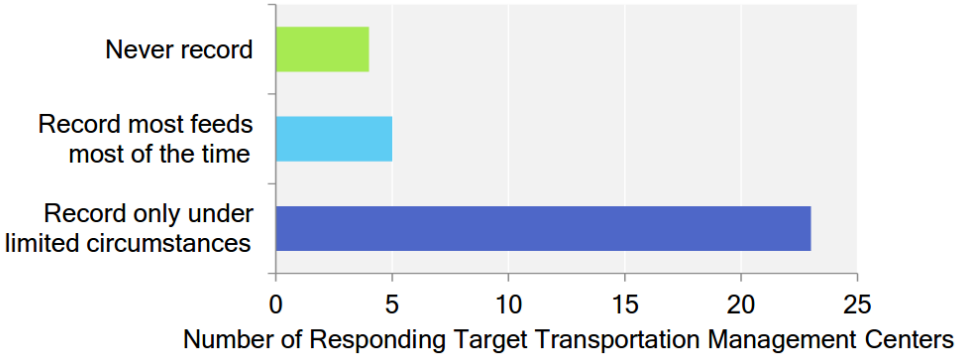


Figure 2: Chart. Recording incoming transportation video feeds.
(Source: Parsons Brinckerhoff.)

While many agencies have recorded under limited circumstances for many years using simple equipment such as a videocassette recorder (VCR), the introduction of networked digital video recorders and inexpensive storage space have reduced the technical barriers to extensive recording. For agencies that see value in additional recording and have applicable operational and legal/policy frameworks, recording most feeds most of the time has become a possibility. For that reason, there is the opportunity that agencies could revisit their decisions periodically and more could shift to the ALWAYS category over time while others could move from NEVER to SOMETIMES.

Best General Practice

While there can be ancillary benefits for having recorded video available as a courtesy to law enforcement agencies, TMC staff need to be clear that the primary purpose of traffic cameras and recording technology is for traffic management.

TRANSPORTATION MANAGEMENT CENTERS THAT ALWAYS RECORD

For those TMCs that are operating under a policy of recording most or all of the video feeds (ALWAYS), the following observations are relevant.

Capability Maturity (Transportation Management Centers that Always Record)

Capability maturity models (CMM) provide a framework for agencies to consider for benchmarking and improving their processes. While there are agency-specific legal, policy, and operational factors that preclude such generalized models from being applicable to all situations, the maturity levels below do draw from the experience of successful TMCs.

Traditional capability maturity models have five

Best General Practice

A great opportunity to review your policy is presented when opening a new TMC, rehabilitating an existing TMC, or preparing for a series of upcoming events.

levels, but to fit this application, they are grouped into three—Initial, Repeatable/Defined, and Managed/Optimizing. The descriptions of each level focus on process and documentation that are generally applicable to TMCs that sometimes record video. Specific tactics within processes, such as a sample file naming convention, are included in subsequent chapters, frequently in the Best General Practices call-out boxes.

Since issues of releasing video clips are similar for TMCs that sometimes record and TMCs that always record except for scale, guidance for release is provided in chapter 3 instead of in this chapter.

Increasing capability maturity is intended to both enhance the transportation management effectiveness of TMCs and to streamline their recording practices. See table 2 for the capability maturity model related to TMCs that record continuously.

Table 2: Capability maturity model for Transportation Management Centers that record most feeds continuously (ALWAYS), focusing on processes to retain specific clips beyond the automatic rewriting time.

Initial	**Repeatable/Defined**	**Managed/Optimizing**
Ad hoc decisions on what to archive, who archives, where files are archived, how files are labeled, and how long they are kept.	Have written policy with how requests to save are made, who processes requests, how saved files are organized and labeled, how the process is documented, and how long files are kept.	Document annual uses of recordings and saved clips including value added and necessary staff time and technical resources to provide; consider needs to revise policies and practices, including reaching out to stakeholders to see if select recordings would support related functions such as engineering studies; consider process simplification.

Additional detail of strategies to support efficient release of recorded video are found in chapter 3.

Length of Time Recordings are Kept for Transportation Management Centers that Always Record

The agencies that always record do so by recording onto media in a continuous loop until it is automatically overwritten after a minimum amount of time. The minimum length of time drives how much storage space is necessary. Agencies recorded a variety of minimum retention times:

- Minnesota: four days.
- Iowa: three days.
- Wisconsin: three days.
- New Jersey: seven days.

Per the Minnesota Department of Transportation's (MnDOT) "Traffic Camera Imagery Recording and Distribution" policy dated December 4th, 2012, retention times vary on the use. The complete listing is as follows:

- Imagery automatically captured and temporarily stored by the system—two to four days.
- Imagery archived by an operator at the request of a government agency for investigation—one year.
- Imagery archived by an operator at the request of the media or the public—90 days.
- Imagery archived by an operator for a research request—may be deleted immediately following its transfer to the requester.
- Imagery archived by an operator and identified as valuable for training or education may be stored indefinitely or deleted upon the conclusion of training.

The same policy also notes that retention times may vary due to factors such as, "system or network health, compression efficiency, changes in technology, or changes to MnDOT's needs."

As shown in figure 3, both storage space and anticipated needs were cited by more than half of the agencies as reasons for choosing the amount of time that recordings are kept by default. That is, the time that the recordings are kept even if specific clips are not saved longer for specific purposes, such as training or study data.

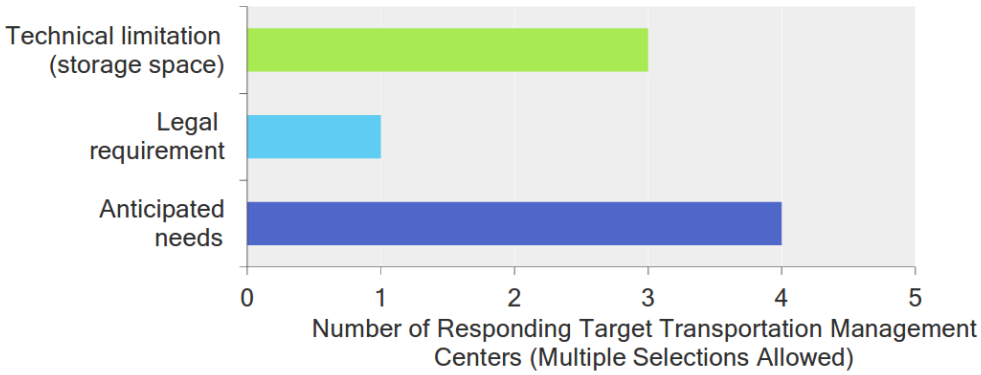


Figure 3: Chart. For agencies that record most feeds by default, basis for length of recording. (Source: Parsons Brinckerhoff.)

The agencies were asked if there was a desire to keep some recordings longer than current storage space allowed. Most respondents indicated that there was not a desire to retain video longer—even if additional storage space was available inexpensively.

TRANSPORTATION MANAGEMENT CENTERS THAT SOMETIMES RECORD

For those TMCs that are operating under a policy of only recording under limited circumstances for specific purposes (SOMETIMES), the following observations are relevant.

An example of an approach for selectively recording video comes from Minnesota in the years prior to 2008 when they started recording continuously. They assessed the needs and opportunities for limited recording and added Digital Video Recorders (DVR) to cover groups of cameras accordingly. For example, when installing a new cable median barrier, they started recording cameras that monitored it. Not only did it record the performance of the barrier for

internal use, but also video was released of a prevented head-on collision when the gentleman who had been saved took to the media to acknowledge the value of the barrier. Minnesota also strategically deployed recording for the change of a High-Occupancy Vehicle (HOV) lane to a High-Occupancy Toll (HOT) lane and monitoring top crash locations.

Capability Maturity (Transportation Management Centers that Sometimes Record)

The Capability Maturity Model in table 3 for TMCs that sometimes record has some similarities to the corresponding one for TMCs that always record (table 4), however, there are important differences as well. Similarities including moving from an ad hoc system through having and following written documentation to performance management and proactive looking to improve and simplify. Another similarity is electronic file organization. However, there are differences in the content that are specific to different needs of TMCs that always record and those that only sometimes record. The tables have been kept separate for the completeness of their respective sections.

Table 3: Capability maturity model for Transportation Management Centers that sometimes record video.

Initial	**Repeatable/Defined**	**Managed/Optimizing**
Ad hoc decisions on which types of events to record, when to start recording, who decides to start recording, and how files are saved.	Have written policy with agreed-upon types of events to record and who has the authority to make and delete recordings; file management system or standardized, searchable file naming convention.	Document annual uses of recordings including value added and necessary staff time and technical resources to provide; consider needs to revise policies and practices, including reaching out to stakeholders to see if select recordings would support related functions such as engineering studies; consider process simplification.

Length of Time Recordings are Kept (Transportation Management Centers that Sometimes Record)

Literature review uncovered that the general practice in a security application of CCTV is to keep recordings for 30 days, though some may choose lesser amounts if a screening process is in-place to know that a recording will or will not be valuable. For traffic management applications, however, outreach to the agencies uncovered a much larger variation in length of time that recordings are kept as shown in figure 4.

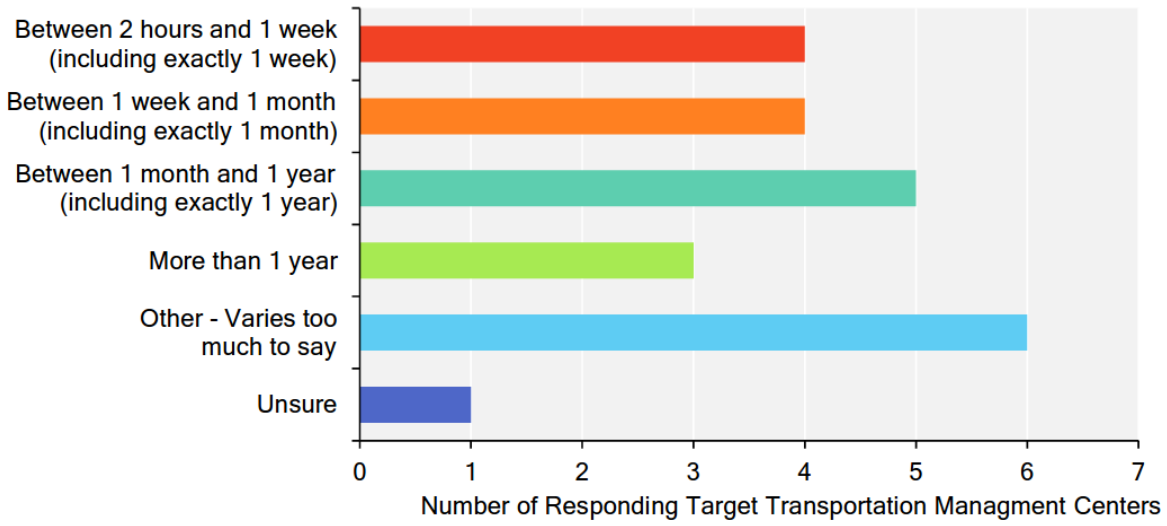


Figure 4: Chart. Length of time agencies that record under limited circumstances keep recordings.
(Source: Parsons Brinckerhoff.)

The feedback received from agencies and TMC operators underscores that the length of retention frequently varies and that it is often influenced by the use of the selected recording. However, across agencies there were no real firm trends; it varied widely even when the anticipated uses were the same.

For training videos, as an example, one agency said that training videos are the only type of recording kept for more than one day. Another agency notes that after-action reviews and trainings are scheduled as soon as possible and that recordings are then no longer retained. Yet another agency notes that there is no specific time duration for keeping training material.

The agencies were asked if there was a desire to record more frequently or to keep some recordings longer than current storage space allowed. Almost three quarters of respondents indicated that there was *not* a desire to record more or to retain video longer. However, some respondents noted that enforcement or other agencies might be interested in more frequent recording or longer retention, but it was beyond their purview. One noted that enforcement agencies could record the live video feed provided to them by the transportation agency.
In addition, there was no correlation in those not interested in recording more frequently versus the length of the time they typically kept recording.

USES OF RECORDED VIDEO FOR SECURITY AND LAW ENFORCEMENT

For traffic management, real-time situational awareness of vehicle flows is the key. For security and law enforcement, records that can be used for evidence are also vital. DOTs now often have large networks of cameras and, policy permitting, they could be recorded. TMCs typically share video with law enforcement agencies and may be colocated with law enforcement agencies. It is important to consider and discuss the differing needs, including operational needs, as well as

legal frameworks when there is this overlap. The New York area Triborough Bridge and Tunnel Authority gave the following scenario as the basis for discussion—a box truck is stopped next to a bridge pier. From a traffic management perspective, the need is to dispatch roadside assistance, monitor queuing, and provide traveler information. However, from a security perspective, there is a need to view the truck closely to help assess if it might be an intentional stop and have explosives. In the latter case, having a record of evidence is crucial. The decision on whether to dispatch a tow truck, law enforcement, or both could rest heavily on the initial use of the nearest camera. Even within a roadway agency, there may be security-focused cameras covering bridge piers and office building doors. For these cameras, recordings are also important for investigations. However, there are different privacy concerns for the doors of buildings since individuals are shown through the normal course of their work.

When knowledge that video is available spreads among local agencies, additional requests occur. New Jersey DOT (NJDOT) once processed a request from a Society for the Prevention of Cruelty to Animals (SPCA) for footage from a temporary trailer-mounted camera that had been set up to monitor a construction detour.

CHAPTER 3: SUCCESSFUL PRACTICES FOR FULFILLING REQUESTS FOR RECORDED VIDEO

The procedures used by Transportation Management Centers (TMC) to respond to requests for recorded video from the public and from other agencies are also of interest to this report. Our findings focus on formal requests, that is, ones that are submitted and tracked. However, some agencies also acknowledged that some requests are handled informally, such as footage for traffic studies that may be given to a research agency and then not retained.

DECISIONMAKING FACTORS AND PROCESS, INCLUDING CHANGING POLICIES

As part of the outreach to agencies, a question was asked seeking the reasons for selecting the main policy choices. Of the 36 metropolitan area TMCs that responded to the inquiry, four of them reported that they never record and all four cited legal and/or policy reasons. One of the agencies believed that the Freedom of Information Act (FOIA) would require recorded video to be available to the public, a requirement that would induce a need for additional staff. A different agency commented that the State's open records law makes recording (such as required by their associated transit agency) very expensive. In response to a follow up on the possibility of revisiting the policy to not record at all, three of the four TMCs saw no need to reconsider the policy given their current understanding of the legal and legislative environment. The remaining agency stated that the FOIA would require additional staff to provide responses and that would drive the policy decision. As discussed later in this report, understanding the different State FOIA and record retention laws is a fundamental step in determining your current situation.

There were five TMCs that reported recording most feeds most of the time (categorized in this report as ALWAYS). Three of them suggested their primary motivation was to provide a buffer (time) to decide whether or not video of specific times and locations might be needed for later use. Video not flagged for longer-term use would be overwritten.

The remaining two TMCs gave the reason for recording all feeds as a policy or legal requirement.

Further discussions with case study agencies delved into how agencies choose their policies.

In 2014, Iowa's Statewide TMC initiated continuous recording of video (ALWAYS). The decision was led by the Executive Director of the Iowa Department of Transportation (DOT) and was based on the desire for recordings to be used in training and after-action reports. There were concerns about staff time for releasing video, especially since staffing was being reduced. Iowa DOT staff consulted with Minnesota DOT (MnDOT) staff, who were also recording most of their feeds and fulfilling requests for video from the public. They learned that fulfilling the requests did not have to be an overwhelming burden when steps are taken to increase efficiency.

In Minnesota, Washington, and Wisconsin, ad hoc recording on select feeds on video home system (VHS) tapes has gradually developed the current practice of recording most feeds continuously. In Minnesota, between 2002 and 2007, several digital video recorders (DVR) were

added to cover groups of cameras for specific needs (such as installation of new cable median barrier, change of a High-Occupancy Vehicle (HOV) lane to a High-Occupancy Toll (HOT) lane, and monitoring top crash locations). Based on the value of these recordings, a confluence of three enabling factors led to the change to recording all feeds in 2008. The three factors were the I-35 bridge collapse which highlighted the need for a redundant IP video backup to the existing analog video distribution network, significant server hardware was available at no cost from another MnDOT unit that didn't need it, and video management software was used for coordinating cameras for the 2008 Republican National Convention. Although some people within the agency had not been in favor of the expanded recording, given the unique needs and opportunities in 2008, it was decided to change the policy. Since then, the value gained has been considered to outweigh the extra work distributing recorded video so the expanded recording policy has remained in effect. Wisconsin started recording most feeds continuously in 2007. The motivation was the value of being able to see and understand the beginning of incidents. The change was implemented as part of the investment in the creating their Statewide Traffic Operations Center (STOC).

Recording policies occasionally reach the media, such as when New Mexico DOT's (NMDOT) policy of never recording was reported in conjunction with a tragic shooting in 2015 in Albuquerque that happened near a NMDOT camera. NMDOT provided the following statement to the media, "Our hearts and prayers go out to the family who lost their little girl to an act of senseless violence. We work very closely with law enforcement agencies to assist in their operations, and we are certainly open to looking into ways to improve how we can better assist them with the resources we have available." Following up with NMDOT for this report, since traffic operations is the primary purpose of the cameras and since recoding all feeds most of the time would be a significant cost, NMDOT is not actively reconsidering their policy of never recording.

Those examples of changing policies illustrate how shifts are more likely when other changes are happening, such as investing in a new TMC or road facility. It is helpful for agencies to consider technical, operational, and legal/policy factors when opportunities to change arise. Each will be covered in more detail in subsequent chapters, but is summarized as follows:

- **Technical—**Storage space/networked video recorders (NVR), video management software, resolution and frame rate.
- **Operational—**Benefits of recorded video, when to record video, staff time to respond to requests to video recording.
- **Legal/policy—**Open records laws, records retention laws, privacy considerations.

PREVALENCE OF RELEASING RECORDED VIDEO

For agencies that continuously record (ALWAYS) or those that only record on limited basis (SOMETIMES), the majority do accept requests for copies of recorded video, either through a FOIA process or otherwise. See figure 5.

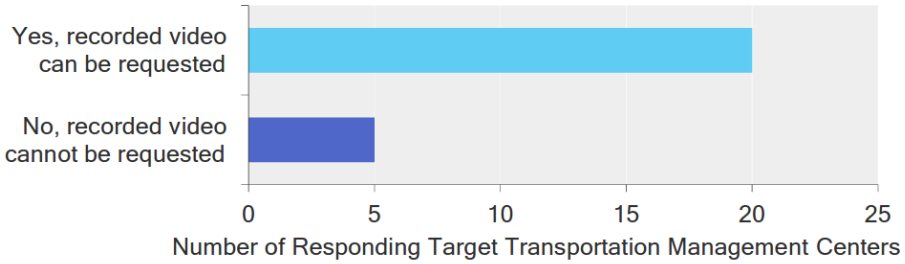


Figure 5: Chart. If recorded video can be requested.
(Source: Parsons Brinckerhoff.)

There was not a correlation between if the recording was continuous and if requests could be made. In Washington State, video is recorded continuously, but the recordings are considered field data that is automatically overwritten and not retained for public records. In Texas, recording is only done for training and video is deleted as soon as the use is complete.

PROCEDURES FOR REQUESTING RECORDED VIDEO

Of those TMCs that do allow formal requests, the requests can come in from the public as well as from enforcement agencies, researchers, agency staff, and through subpoenas. While accepting requests from the public could be required by the State versions of FOIA, several agencies have developed request procedures outside the agency's FOIA contact for other agency records. The alternate request processes seem to allow quicker turnaround when the automatic recording time is limited.

Table 4 provides three examples of video request procedures that demonstrate the wide variability in providing recorded video. Unlike most agencies, the three in the table posted the procedures online.

Best General Practice

For recorded video requests, consider having an efficient process that includes:

- The same Web-based request form for public and law enforcement requests.
- Integration of the Web-based form to a database that tracks request disposition.

Table 4: Select video request procedures.

	New Jersey Department of Transportation[1]	Iowa Department of Transportation[2]	District of Columbia Department of Transportation[3]
Request Media	PDF form via emailed	Web form	Web form (preferred), mail, fax, email
Request Made to Freedom of Information Act (FOIA) Officer?	No	No	Yes
Length of Time to Request from Date of the Recording	7 calendar days	3 business days	10 calendar days
Fees	$100 for first 3-hour period and $50 for each additional 3-hour period	None	None

Notes:
1. Source is http://www.state.nj.us/transportation/business/videolog/faq.shtm.
2. Source is http://www.iowadot.gov/511/trafficcameravideorequest.html; Link used by enforcement and public (not directly linked from Iowa DOT Web site).
3. Source is http://hsema.dc.gov/page/open-government-foia-and-cctv/.

METHODS OF FULFILLING A VIDEO REQUEST

Methods of fulfilling requests for video vary across agencies. Even with agencies, there can be different practices for more formal requests, such as those tracked through FOIA, and less formal requests, such as data for traffic studies. Since procedures are highly dependent on agency legal, operational, and technical frameworks, there is not a single best practice. Two examples are provided to give agencies ideas on various parts of the process to consider when developing or revising their own methods.

The New Jersey Department of Transportation (NJDOT), an agency that records most feeds most of the time, reported the following process and notes:

- Senior TMC staff in each TMC is assigned to process video requests.
- The initial screening of requests are checked to see if they are within the published timeframe of how long video is kept, if the request contains the required location information, if the location is within the agency's jurisdiction, and if the request is an area covered by a closed-circuit television (CCTV) camera.
- Many requests, particularly from the public, are well beyond the published availability or have referenced cameras that are actually video detection cameras.
- When relevant video is found through the agency's video management system, it is either burned to a digital video disk (DVD) or arrangements are made to transfer to a flash drive.
- The agency converts the video to Microsoft's Advanced Systems Format (ASF) prior to release.

- Requests from the public, including their lawyers, are assessed a fee according to a published schedule. Requests from other public agencies, such as law enforcement agencies, are not charged.

Initially, NJDOT released clips in the agency's video management system's proprietary format with the copy of the video management system's video player. However, many recipients had difficulty accessing the video.

The Wisconsin Department of Transportation (WisDOT) provided the following fulfillment procedure:

- Request called into control room or Archive Video Administrator.
- Operators obtain requestor's information, check if video available, save any found video, and enter into database.
- Archive Video Administrator notified of request, approval obtained from DOT and law enforcement (if needed).
- Archive Video Administrator burns video to a DVD. If the request is too large for a DVD, other media can be arranged.
- Requestor contacted to pick up the video. There is no cost to requestors.

Wisconsin's in-house information technology (IT) staff wrote a helpful program to track requests for video.

Best General Practice

Keep the request process simple and scalable. Consider using forms linked to tracking databases when possible to prevent repetitive manual data entry.

IMPACTS ON TRANSPORTATION MANAGEMENT CENTER STAFFING LEVELS

Through the literature search and conversation with agencies, it is understood that the potential burden of responding to requests for video when feeds are recorded continuously was an important factor to some agencies.

The online inquiry asked about what kind of burden responding to these requests might impart, there was a wide variety of experience displayed by this outcome. While more agencies perceive the burden as low than as high, either having few requests or having many requests can lead to a high burden depending upon available resources. Figure 6 shows the responses:

Figure 6: Chart. Burden for responding to requests for recorded video.
(Source: Parsons Brinckerhoff.)

MnDOT's Regional TMC (with about 760 cameras recorded for four days) classified the burden as low to medium with many requests, but adequate staff resources. Over the last year there has been an average of four inquiries per day requiring approximately 1/5 full-time equivalent (FTE). Importantly, there has been an increasing trend in the number of requests, nearly tripling since 2010. The totals include mail, phone, email, and written inquiries from the public (including insurance and lawyers), internal agency requests, and law enforcement requests. The same agency also notes that the majority of requests from the public cannot be fulfilled because they are submitted too late, pertain to events not visible on the camera, or pertain to a location not covered by a camera. The public often perceives that the traffic detection cameras are recorded or that they are red-light enforcement cameras.

For Wisconsin's STOC (with about 300 cameras recorded for 72 hours), the Archive Video Administrator spends an average of 6 to 8 hours per week processing up to four requests per day each taking 15 to 60 minutes. The agency considers this a low burden; while there are many requests, there are adequate staff resources.

As discussed further in the FOIA section below, the public information law itself typically covers release of records that exist, not if records need to be maintained or for how long.

Best General Practice

If most camera images are available through a traveler information Web site, direct petitioners to check if there is a camera in their area of interest and if so, to refer to it in their request. Seeing the level of detail may also help manage expectations for video quality.

Several agencies noted that the probability of having the desired images may be low. Even for agencies that do record most feeds most of the time, the camera may not have been pointed in the direction of interest. Also, the video quality that is sufficient for traffic management use may not be sufficient to be useful to requestors desiring it for other purposes.

Best General Practice

Since video requests coming from law enforcement agencies can comprise 50 percent of the requests, consider assigning fulfillment of video archive requests to a partner law enforcement agency:

- Faster response to their requests w/enhanced chain of custody for evidence.
- Release is not a core traffic management function.
- Some video requires law enforcement approval to release once their investigation is complete.
- Have mechanism to collect fees that offset costs.

Consider, also, the potential risk of perception of DOT cameras used for enforcement

A few agencies noted that requests can be denied, though only under specific circumstances, even when the recordings sought do exist. One example is if video is still under law enforcement investigation. Other examples include critical infrastructure, students in a student setting, and security.

One potential mitigation to the time required for processing requests for recorded video would be to assign the task to operators during off-peak hours. However, agencies such as Iowa DOT, noted a few risks in that strategy. One is that the operators could be subpoenaed to testify in court if they actually copied the video rather than a supervisor. Also, the more people who have access to the files as they are processed, the harder it may be to defend the integrity of the video when used as evidence.

Another potential mitigation to staff time needed to fulfill requests for recorded video where a large portion of requests come from law enforcement would be to have a law enforcement officer access the video system directly to process requests. As noted in the Best General Practice on the topic, there are several potential benefits. However, there is also the risk that public perception of use of DOT cameras for enforcement would be detrimental. Even if law enforcement are just using the video as evidence to support crash investigations, some agencies have expressed a desire to keep the DOT video archive system under their own control.

There are more consensuses on mitigations that reduce the time to process each request, such as the linked tracking forms discussed in the previous section.

CHAPTER 4: SUCCESSFUL PRACTICES FOR SHARING REAL-TIME VIDEO IMAGES

Successful practices were identified to mitigate the risks and deal with the constraints associated with sharing real-time video images with other agencies and with the public.

While this chapter focuses on sharing video outside of a roadway agency, it should also be noted that mobile availability within the agency is increasingly used. Not only are operations staff using the images while managing onsite, some agency executives appreciate being able to view key images on tablets during high-profile events.

Examples, such as the 2008 Republican National Convention in St. Paul, Minnesota, and Super Bowl XLVIII in the New York/New Jersey area have been catalysts to expanding sharing of real-time video, overcoming not only technological barriers, but institutional resistance and the need to work out legal issues between agencies as well.

BENEFITS OF SHARING VIDEO

The classic benefits of sharing video are traveler information and enabling traffic management by sharing video information with regional agencies. From the research with the agencies directly, 31 of 32 Transportation Management Centers (TMC) represented in the online inquiry shared live video or snapshots with at least one other entity. They were asked with whom they share, and the results can be found in figure 7.

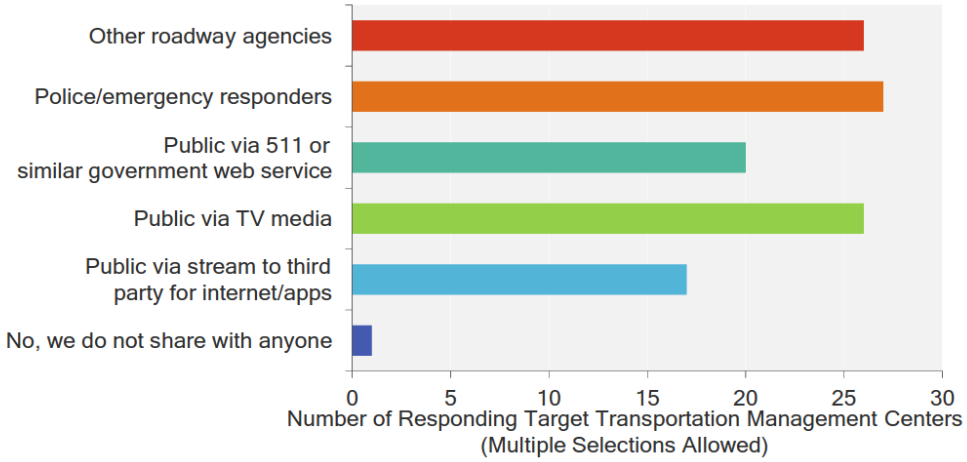


Figure 7: Chart. Recipients of shared video.
(Source: Parsons Brinckerhoff.)

Sharing with the media was a common result, and many agencies have agreements in-place regarding who pays for the communications connectivity, how the video can be used, and how the agency will receive attribution for the video.

Best General Practice

To support Transportation Systems Management and Operations (TSMO) collaboration with local agencies:

- Use recent, local clips in TIM training.
- Offer to share requested clips with local agencies, even if they do not have streaming access.
- Consider including TIM participation as a condition of sharing streaming or recorded video.

It should be noted that sharing with the public on the Internet takes many forms, including streaming video and snapshots (sometimes even within the same agency). Some cameras will stream for a short time and then need to be refreshed. Some agencies only share a subset of their cameras. There are also businesses established that are under contract with agencies to help stream their video over the Internet.

As an example, Houston TranStar, a consortium of governmental agencies serving the Greater Houston Region, provides static images on its traveler information Web site and streaming video to the media, noting, "Offering live video over the Internet from our 600-plus cameras would require tremendous technical resources and diminish the level of service we are able to provide from the rest of our systems. Each media outlet has a single video feed from our system and can typically provide streaming video from only a single camera at a time." (http://traffic.houstontranstar.org/faq/webfaq.html accessed 5/28/15).

The Federal Highway Administration's (FHWA) Traffic Incident Management (TIM) program calls out the importance of sharing video and data among agencies as well as the importance of sharing real-time traveler information with incident-specific information.

In the 2003-2014 TIM self-assessments (SA), there are questions in both of these areas.

- For sharing data and video, the relevant question numbers are 4.3.1.2 in 2003-2008 and 2011-2013 and 4.3.1.3 in 2009-2010.
- For real-time motorist information, the relevant question numbers are 4.3.3.2 in 2003-2008 and 4.3.2.1 in 2009-2013.

These questions do not differentiate between video feeds and other data, though. That aside, there is definitely a trend of increased video and data sharing. Among agencies reporting on their TIM SA there is an average increase in the response value to the video and data sharing question (4.3.1.2) of 138.4 percent and increase in the response value of the motorist information question (4.3.2.1) of 86.6 percent between the baseline and 2013 assessment (2013 *Traffic Incident Management National Analysis Report, Executive Summary*, FHWA, November 2013).

The 2015 TIM SA has a significantly revised question list and will set a new baseline. There are separate questions for data and video sharing, 48 and 49 respectively. Question 49 focuses on sharing video with other agencies, but also mentions sharing of video that is also available to the public. The full text of question 49 is, "Is TIM video captured via TMCs and/or public safety CAD [computer aided dispatch] systems and is it shared with other disciplines for real-time operational purposes?" Question 49 has the following responses with corresponding scores:

- Score 1 if No TIM video is collected and shared.
- Score 2 if some TIM response agencies can access State Department of Transportation (DOT) video but only via methods available to the public (e.g., 511, Web sites, etc.). No video originating from public safety CAD systems is shared with DOTs or there is strong reluctance to do so.
- Score 3 if TIM-related video is collected by DOT and public safety agencies and is shared by some, but not all, responding agencies. Some agencies are not aware of video sharing capabilities or don't routinely utilize video for operations.
- Score 4 if TIM-related video is routinely and automatically shared among all responding agencies and is fully integrated into public safety CAD and DOT traffic management systems. Video is routinely used to tailor response and for other operational purposes.

Note that the TIM scores do not mention video recording specifically.

Another benefit of sharing video related to TIM is building relationships with local emergency responders. New Jersey noted offering recorded video of incidents from DOT cameras within their jurisdictions. It is also impactful to start TIM training sessions with recent video of an incident that occurred nearby.

According to the Tennessee Department of Transportation (TDOT), "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." (Access to Live Video Feeds and Information Sharing, undated; see appendix.)

Another benefit of sharing video with the public is showing that State DOT investments are being useful.

CONSTRAINTS, RISKS, AND MITIGATIONS OF SHARING VIDEO

This section covers the reasons that limit sharing by some agencies for some purposes. It also discusses risks and potential mitigations. It is recognized that constraints vary by TMC/agency and that some may be outside the control of TMC staff or even the transportation agency.

Privacy Concerns

New York State captures the balance between function and privacy as, "[Closed-circuit television (CCTV)] systems are data/information-collecting tools. They must be utilized in a consistent manner that strives to uphold the

Best General Practice

For sensitive situations, have the capability to cut feeds to the public/media while preserving them to transportation agencies and emergency responders. If not possible, have a camera use policy which includes not zooming into personally identifiable details.

public's expectation of privacy, while serving their function as a traffic management and traveler information tool." (Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems, September 4, 2001.)

Agencies have differing views on the details of privacy, but there are some generally used tactics to protect identifying information of individuals. One technological approach is to only share relatively low-resolution images with the public. One operational method is instructing operators not to zoom into crash sites. There is also the combination technological and operational approach of giving TMC operators the capability to selectively cut feeds to the public when zoomed view is necessary for emergency response, such as zooming in to read a hazardous material placard. Additional detail on addressing privacy concerns is available in chapter 7.

Technical and Communications Issues

Best General Practice

Make sure that your IT department:

- Understands changing needs for traffic video, such as providing secure access to video for the media.
- Knows that equipment, software, and services exist to help with emerging needs.

Digital and Internet Protocol (IP) technologies continue to improve with implementation of newer video compression techniques allowing higher quality video to be distributed and potentially archived with less communications bandwidth. Further, the networks themselves continue to improve allowing for higher bandwidth capability both for video being transmitted to the TMC itself as well as for distribution to other centers, users, or even the public. Again, it is not uncommon for video being shared to the public or other centers to be of lower quality or format to allow more users additional access. Conversion of real-time video for large-scale distribution can be expensive and require considerable information technology (IT) infrastructure.

The IT department in the Tennessee DOT determined that the legacy access provided by the media for streaming video was not secure enough. That need, along with the needs to provide access to local agencies inexpensively and to provide easy video access for senior team members for events, prompted procurement of a new software solution to handle video sharing. It includes modules for media access, emergency responder access, and an executive view portal.

Some agencies, such as the Minnesota Department of Transportation (MnDOT), use stills for real-time instead of full motion due to bandwidth constraints.

Legal, Policy, and Institutional Issues

Most agencies have policies in-place for sharing images with the public—some written, some institutional. These policies will sometimes be structured around sharing all cameras or just a subset. When sharing with the media or with a privately operated travel information Web site/service there can be legal arrangements with an intermediary (third party). Also, costs typically increase with sharing more cameras, higher frame rates, and higher resolutions. A

private hosting and streaming service or next generation video management technology can mitigate costs.

When it comes to sharing images with other agencies, including roadway agencies, law enforcement entities, and other first responders, again, most organizations are willing to work a little harder to resolve any differences to ensure maximum operational sharing—even if it means working out issues such as camera control. Policies also recognize today's TMC operating as a clearinghouse and often address video ownership. For example, the Niagara International Transportation Technology Coalition (NITTEC) is a clearinghouse for images from multiple agencies, including agencies in two countries. Its CCTV policy notes that it does not supersede the policies of individual agencies. For many agencies, a Memorandum of Understanding (MOU) needs to be executed to share video.

For sharing with agencies and with the public, there can be institutional issues of working through the agency IT department. As one head of intelligent transportation systems (ITS) design once said, "Working with IT is harder than raising the dead." Thankfully, not all agencies have such challenging relationships with their IT groups. However, differences in goals and priorities can lead to stumbling blocks. Also, the ITS systems in some agencies originated outside the purview of IT departments leading to territory issues. IT is essential, though, both for the functioning of the connections and for maintaining network security.

SHARING WITH LAW ENFORCEMENT AGENCIES AND SECURITY GROUPS

Sharing video with law enforcement agencies adds value to incident response. Some cameras are positioned in view of both traffic and infrastructure. Some cameras that don't view traffic, such as under bridges monitoring the piers, also share the same communications network. The potential risks to consider are mainly laws or funding requirements that could separate the functions. Automated enforcement is typically kept completely separate from traffic management since there are privacy concerns and strict evidentiary rules.

Best General Practice

Be clear that the primary purpose of sharing video with law enforcement agencies is to assist with incident management. Additional uses of video by law enforcement agencies and security groups need to conform to applicable laws and policies.

However, using traffic video to investigate erratic driving complaints or backup law enforcement reports of drive-offs from traffic stops could be less clear.

New York State DOT (NYSDOT) articulates their take on the shared use of CCTV between traffic management and law enforcement as follows:

> "CCTV systems should be designed and used primarily for the traffic management and traveler information purpose for which they were installed and for which the public would reasonably expect. Enforcement agencies play an important public safety role in incident management activities. Accordingly, the Department partners and sometimes

> colocates at TMCs with enforcement agencies to provide for the best incident management service to the public. As a result, enforcement agencies may have access to CCTV data directly or remotely through TMCs for the purpose of coordinating incident management and incident-related public safety activities, and such is not provided for routine or regular monitoring for enforcement purposes. The ongoing sharing of data with enforcement agencies shall be documented by written agreement containing privacy protection language consistent with statewide regulations and this policy. Enforcement agencies shall be responsible for ensuring that any use of the CCTV systems is done in accordance with statutory authority, appropriate legal process, or emergency circumstances as defined by law." (Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems, September 4, 2001.)

New York State's approach highlights the need to discuss and document the sharing of video images used by and for law enforcement.

CHAPTER 5: TECHNOLOGY ISSUES

KEY VIDEO RECORDING TECHNOLOGY ISSUES

Closed-circuit television (CCTV) camera and management systems, as with much of today's technology products, continue to improve over time with each successive generation. Innovation in the consumer and security technology spaces drive progress, enabling enhanced flexibility and capabilities for the transportation market including video recording and archiving.

Each generation of CCTV camera that comes to market is integrating new capabilities that previously required external infrastructure and processing capability for typically the same cost within the camera body itself. Key improvements include:

- Enhanced video resolution for better clarity.
- Thermal capabilities.
- Low-light or night-vision capabilities.
- On-board video analytic capabilities.
- On-board video recording.

In general, security-related applications from the commercial space are driving these technology improvements with focus on improved video clarity, analytics, and recording capabilities. A key enabler of these enhancements is the rise of Internet Protocol (IP) based video systems. Legacy video systems were largely developed around analog technologies effectively forcing a centralized architecture of field cameras to a central video switch at an operations center for local distribution and archival ability. With the advent of digital cameras and IP technologies, the ability to distribute and share video is greatly simplified. The technology infrastructure is largely distributed with multiple users having the possibility of accessing video from multiple destinations be it a video wall, workstation, network storage or even a cellular phone.

Management systems also continue to improve offering updated user interfaces with additional capabilities and flexibility. Coupled with the implementation of IP video systems, a greater opportunity for video recording and archiving has been enabled. Early analog systems utilized commercial-grade tape-based recording devices recording in a loop. With the transition to digital and IP-based technologies, network storage systems containing video files are now less complicated. Today, depending on the communications infrastructure and design of the system, a single camera can provide a high-quality video stream to an operator with a lower quality stream being provided to a distribution or archival server while at the same time keeping a copy of the stream on storage media on the camera or local video encoder in the field. That archived video and the higher-quality real-time video itself can be accessed and distributed to a variety of users obviously dependent on user rights.

Digital and IP technologies also continue to improve with implementation of newer video compression techniques allowing higher quality video to be distributed and potentially archived with less communications bandwidth. Some transportation agencies have noted that video compression can struggle with grid images, such as open grate bridge decks and bridge trusses.

Sizing hardware, software, and data storage for a video archival system is related to the number of cameras being recorded, the quality of the recorded video stream, and the sizing and availability of the communications network in use. Video archive contents can vary from simple intermittent single images to full video clips stored over time. The appropriate hardware to support this range of capabilities varies accordingly.

One agency that stores most feeds most of the time provided some information to give a scale of the technical resources required. In the Wisconsin Department of Transportation's (WisDOT) 2013 "CCTV's Role in WisDOT TIM [Traffic Incident Management] Success" webinar, it states that for a system of nearly 300 CCTVs (most at 1.5 megabits per second (Mbps) transported via Internet Group Management Protocol (IGMP) multicast), they use seven networked video recorders (NVR) to keep a 72-hour continuous loop of each feed plus temporary storage for up to 120 days of selected clips. Each NVR contains 12 terabytes of storage, costs approximately $18,000, and lasts for 3 to 5 years. WisDOT currently has approximately 400 cameras.

Best General Practice

When saving video clips, use a consistent and searchable file name structure to save time and improve accuracy. An example is:

[DATE] [TIME VIDEO STARTS] [APPROXIMATE LOCATION] [EVENT TYPE] [CASE NUMBER] [NAME OR BADGE OF REQUESTOR] [CAMERA NUMBER OR MONITOR OUTPUT].avi

On the operational side of camera recording technology, the more video is saved, the more important it is to efficiently be able to access clips. Video management software is the primary tool for accessing clips efficiently. However, it is also sometimes necessary to save files outside the software, such as records of fulfilled requests. The Minnesota Department of Transportation's (MnDOT) Regional Transportation Management Center (TMC) identified the best practice of having a consistent and searchable file name structure, shown on the right.

EMERGING TECHNOLOGY

As stated previously, the march of technology continues at an ever increasing speed. Consumerization (the promotion of the interests of consumers) of many IT-related industries drives this trend even further as many of the technologies necessary for transportation-related CCTV systems have analogues in both security and the consumer spaces.

Several trends in CCTV cameras recently should be noted. Many encoders and digital cameras have capabilities enabling streaming of multiple video

Best General Practice

To mitigate the risk of high cost to store large volumes of data for video, generate two streams from each camera:

- Higher resolution or frame rate for live viewing.
- Lower resolution or frame rate for recording or sharing.

streams in varying qualities enabling high-quality real-time feeds for operators with lower-quality feeds provided to distribution or archival systems. One tactic to balance needs and costs is generating two different streams at the camera or encoder.

Most authorities operating TMCs in Australia use the following dual streaming strategy:

- For operators viewing live feeds, high resolution at 25/30 frames per second (fps).
- For archiving, low resolution at four fps.

TMCs can also manually activate recording on the high-resolution stream when needed.

Many cameras and encoders also enable capture of intermittent or event-based image captures for storage or use in traveler information systems. Simply put, the camera or encoder can store snapshots captured from the encoded video stream either locally on the device via on-board or flash card storage or on a network storage device at the TMC. These snapshots are taken based on parameters set by operators, such as time-based or event-based. For security applications, examples of events to trigger recording would be door openings or vehicles parked in specified areas. For traffic management, events to trigger recording could be wrong-way vehicles or stopped vehicles. These capabilities allow increased archival capabilities while limiting the necessary storage space on network drives and recording devices. Note that while video analytics have great potential beyond vehicle detection, they have reliability issues for some outdoor applications.

Another trend in camera technologies is the rise of very high-resolution cameras. As an individual camera this is of limited utility given many video walls and computer displays cannot display the full resolution of the stream. That said, with appropriate lenses one camera could in fact support a much broader field of view at the same level of detail and quality as multiple cameras. For example, video detection systems that traditionally require cameras on each approach to an intersection can be replaced with a single camera capable of observing all approaches. An example is in figure 8. The original image is in the lower left hand quadrant. The remaining three images are portions of the original that have been stretched to more clearly show the various parts of the intersection.

Figure 8: Screenshot. Composite from wide-angle camera.
(Source: GridSmart)

These types of cameras may seem to have limited use for a typical highway application but coupled with incident detection analytics a single camera can provide operational awareness for all angles in viewable range of a camera location without having to pan the camera. From an archival perspective, the video storage requirements for this type of camera would be higher and may require specialized viewing software.

Communications and archival storage systems continue to progress along with the trends within the information technology (IT) market. Multigigabit communications capabilities suitable for long-distance fiber have become less expensive and more prevalent in field intelligent transportation systems (ITS) networks enabling higher bandwidth uses of video. Network storage capacity continues to become less expensive over time as that market continues to mature. Standards within the video market continue to develop enabling additional compatibility between various vendor elements such as cameras, encoders, and video walls. Standards should be considered as legacy systems are updated.

One innovative recording strategy uses sound to automatically trigger saving video clips before, during, and after crashes and misses. The Traffic Response and Incident Management Assisting the River Cities (TRIMARC) in the greater Louisville and Southern Indiana area used a system called Auto Incident Recording System (AIRS) as part of a program to improve safety at intersections. More recently, the system has been used by the Roads and Traffic Authority of New South Wales at locations in Sydney, Australia. One primary benefit of the system is being able to gather misses which are not reflected in law enforcement reports, while other benefits of capturing incident and training video are more obvious.

RELATION TO SECURITY AND LAW ENFORCEMENT USES

Given the widespread deployment of CCTV to support transportation management and law enforcement, there are opportunities for differing policies related to video archiving and management. Video management systems typically have the capability to limit access, control, and even specialized functions such as recording on a user level. Therefore, law enforcement could have access to a transportation-specific video stream and archive that stream based on their policies without affecting TMC policies. Further, a TMC might have access to a law enforcement or security video stream and not have control or be blanked out during an event. Obviously, these types of details should be subject to memoranda of understanding (MOU) and other appropriate agreements between agencies as this distribution is enabled.

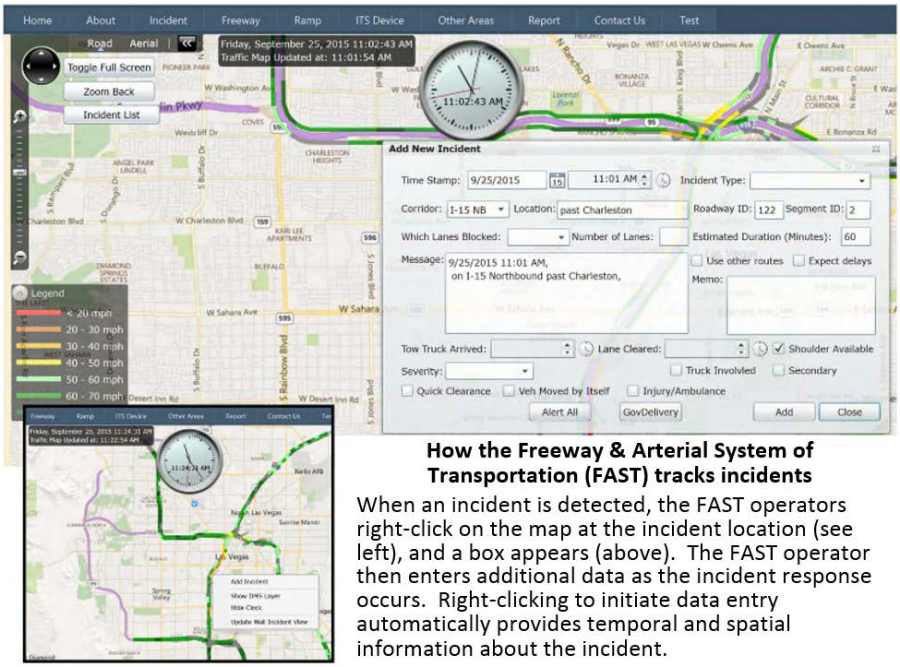
ADDITIONAL IMAGE DOCUMENTATION TECHNIQUES

Image capture techniques vary and can be implemented at many points in a video system. Many digital cameras or encoders have the capability to capture intermittent video images and store on the camera or encoder or transmit them to a network share. This could be triggered from an analytics package or via a time-based setting. Management systems often have the capability for a user to take a screen shot of video playing on a workstation as well.

Best General Practice

Consider a software feature to allow TMC staff to associate multiple camera feeds with an incident and automatically record a composite screenshot at a predefined interval that can later be reviewed for incident clearance performance management.

The Regional Transportation Commission (RTC) of Southern Nevada uses a customized screen capture system as part of an innovative program to utilize their camera network. Their central software allows technicians to right click on the map to create an incident record (figure 9; see larger copy of image in Section 0; the Freeway and Arterial System of Transportation (FAST) is a TMC within the RTC of Southern Nevada system).



How the Freeway & Arterial System of Transportation (FAST) tracks incidents

When an incident is detected, the FAST operators right-click on the map at the incident location (see left), and a box appears (above). The FAST operator then enters additional data as the incident response occurs. Right-clicking to initiate data entry automatically provides temporal and spatial information about the incident.

Figure 9: Screenshot. Regional Transportation Commission of Southern Nevada screen shot—incident tracking.
(Source: Regional Transportation Commission of Southern Nevada)

One of the tabs allows users to populate a 3x3 grid with nearby cameras. Using a custom script, a composite of the images is recorded every 15 seconds for the duration of the incident (figure 10 below, left side). The window includes playback controls (see larger copy of images in Chapter 8.)

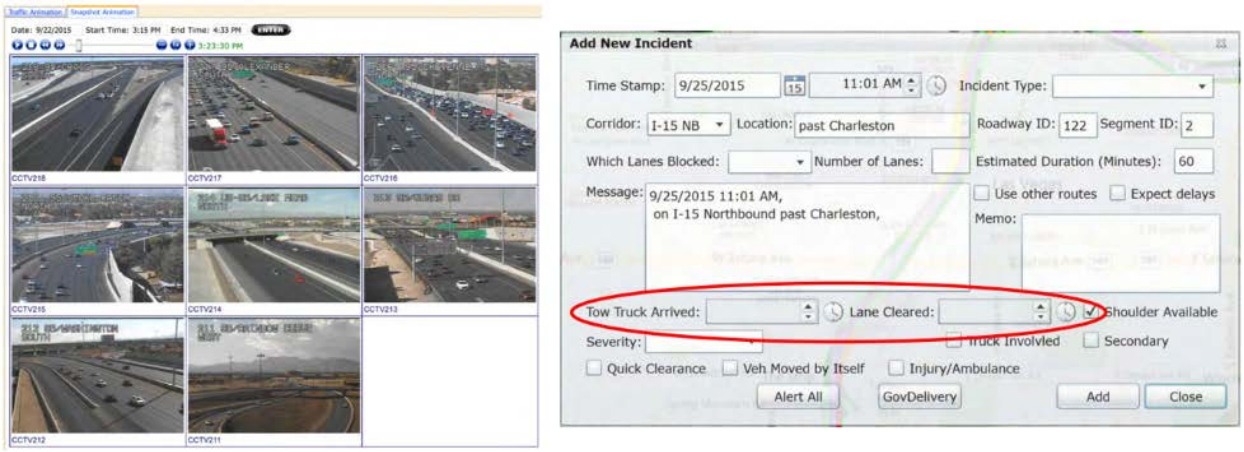


Figure 10: Screenshot. Regional Transportation Commission of Southern Nevada screen shots—incident screen capture matrix and data record.
(Source: Regional Transportation Commission of Southern Nevada)

The images can be reviewed later to collect key incident clearance events (see figure 10 above, right side.) The images also reveal length and dissipation of queues.
Southern Nevada RTC's policy is not to record at all, but their screen capture techniques could be used by agencies that continuously record, sometimes record, or don't record at all. The system makes targeted sets of information that are easy to find and review while taking less storage space than full-motion video.

VIDEO MANAGEMENT SYSTEM CONSIDERATION CHECKLIST

Table 5 lists items that agencies should consider before making changes or upgrades to their video management system. These items are a first step for having informed discussions with agency IT staff as well as vendors, consultants, and other trusted advisors.

Asking, and answering, these questions will begin with establishing the purpose of the live, shared, and/or recorded images. Examples of purposes are included in this report, but ultimately, each agency leadership drives a vision. The purpose and intended operations dictate initial requirements. Some questions within this list examine current video and network assets, a critical step towards assessing gaps and the feasibility (technical and financial) of making improvements.

An example of the importance of purpose in technical decisions is storage. It is one thing to establish a duration of saved video. It is another to determine the technology. Take the question, "Is failover storage required?" At one end of the spectrum is hot failover at two locations—nearly instant redundancy. The other end could be a single drive that needs to be manually replaced or fixed, leaving a gap in recording. For a high-security application, the extra costs of the hot failover may be justified. For recoded video as a courtesy, something like a redundant array of inexpensive/independent disks (RAID) at one location may be appropriate.

Table 5: Video management system checklist.

Topic	**Question/Consideration**
Cameras	Existing camera inventory including: Internet Protocol (IP), analog – pan-tilt-zoom (PTZ), analog (fixed); Format; Compression; Bandwidth; Frame Rate; Resolution; Brand; # Feeds per Camera (hi/lo); Historic Average Bit Rate; Brand; Age
	Timeline to replace/upgrade cameras and characteristics of planned cameras
	What is the total maximum number of cameras for the system?
Network	Unicast or multicast?
	Connection type(s) (how are devices connected to aggregation point(s)? If local area network (LAN), connected to statewide central wide area networks (WAN)?)
	Do cameras come back to a single or multiple locations?
	Upload/download bandwidth allocated for IP video?
	Who operates and maintains the field network?
	Is the central network Department of Transportation specific or statewide?

Table 5: Video management system checklist (continued).

Topic	Question/Consideration
Network (continued)	Who maintains the central network?
	What security rules are there for network access?
	Who maintains the central network?
	What security rules are there for network access?
	Is there a firewall between the field and central networks?
Storage	Centralized or distributed?
	If distributed, number of storage sites? For each site, how many cameras and which types?
	Days of video storage desired?
	Days of video storage required?
	Is storage size maximization most important (budget) or data protection/reliability most important (reliability)?
	Is failover storage required?
	Is dual location, simultaneous recording desired?
	Is video analytics required, and if so, what type and on how many cameras?
Management including Sharing	Is centralized system/user management desired?
	What integration is expected with current or near-term proposed systems—Advanced Traffic Management System, video management system, video walls?
	How many workstation personal computers (PC) online simultaneously?
	Mobile/remote connectivity desired? What is the remote mobility expectation of the customer? Phones? Laptops? What is the connectivity speed for remote users?
	Who does the agency want to share video with? What types of devices and systems do they use? How many potential users?
	Does this end user have a virtualized server environment? If yes, is the information technology (IT) department willing to consider putting the video applications on their virtual system?
	What are the expectations for archiving capabilities, including ease of search for archived clips?
Business Case	Is this project or end user value driven or performance driven?
	Is the end user's IT department an integral part of the decision/ownership or is this dominantly security driven?

Note: Most questions were adapted from the "Bosch Video Management System (BVMS) Decision Assistant" rev November 2014 provided by Chesapeake and Midlantic Marketing and expert input from Skyline Technology Solutions.

Many IP cameras have dual stream outputs, something that can be very helpful for viewing live video at a higher quality than stored video. Even if an agency is only using one stream now, it is important to check if existing cameras have the capability and consider including it in specifications for future cameras. Agencies should note that National Transportation Communications for ITS Protocol (NTCIP) for cameras to date is not geared to IP cameras, limiting compliant vendors.

Bandwidth can be a limiting factor for many agencies, whether from device to aggregation point, through an agency network, or sharing with other agencies or the public. There are several factors that influence the bandwidth that images from a single camera will require including compression, resolution, frame rate, and if they are configured for unicast or multicast. Multicast is more bandwidth efficient because in multicast, the same bandwidth is used regardless of the number of receivers (like a radio station) whereas unicast is separate parallel one-to-one streams (like individual phone calls). However, a truly multicast network environment requires extensive configuration and appropriate equipment, not only cameras from switches. By assessing existing network capabilities, agencies with limited bandwidth to meet their viewing and sharing goals can begin to decide which ways to conserve bandwidth, such as changing compression or upgrading to multicast, are more efficient.

CHAPTER 6: LEGAL AND POLICY ISSUES INCLUDING THE FREEDOM OF INFORMATION ACT

The policies that agencies and Transportation Management Centers (TMC) adopt regarding video recording must be within their applicable legal contexts. Since the legal issues vary by State, this section identifies issues, provides general information, and gives recommendations on how agencies can seek the knowledge they need to make informed decisions on portions of policy and procedure that are within their control.

Public information laws directly influence most TMCs that record video. Legal and/or policy concerns were also given as reasons not to record by each of the agencies that stated never recording, with two of them commenting specifically on public information laws. In the words of a representative of an agency that only records under limited circumstances, "It would be a different world if we didn't need to worry about legal." In two States, representatives for agencies that record on a limited basis indicated that requests for video were not allowed, even under Freedom of Information Act (FOIA) laws. However, the remaining TMC representatives did have some degree of burden addressing requests. Directly or indirectly, this issue appears to have some impact on almost every TMC with regard to decisions on recording and sharing video.

Ask your state's Department of Transportation (DOT) office that handles FOIA requests how it processes release of video. If they do not know, ask them to check with their peers in other departments within the State.

This project did not uncover any instances of legal impetus for maximum allowable downtime of camera or recording systems. The recordings are not safety critical. Some written policies, such as the Minnesota Department of Transportation's (MnDOT) and the Tennessee Department of Transportation's (TDOT), specifically say that video is not guaranteed.

FREEDOM OF INFORMATION ACT

The Federal Freedom of Information Act (FOIA) passed in 1967 is designed to give citizens access to Federal records supporting their rights to know about the functioning of the Government. Since the Federal FOIA only applies to Federal records and the Federal Government does not run TMCs, FOIA itself does not apply to TMCs. However, all 50 States and the District of Columbia have public record laws with a similar intent. Some States use FOIA in the name of their own laws, such as Illinois FOIA. Others use different terminology, such as the Alaska Public Records

Best General Practice

Since FOIA and record retention laws differ for all States, ask your DOT's Counsel if your State's FOIA equivalent law has language on video recordings and if differentiates between "raw data" and "records."

and Recorders statute; the California Public Records Act; the Hawaii Uniform Information Practice's Act; the New Jersey Open Public Records Act; the Oklahoma Open Records Act; and the Pennsylvania Right-to-Know Law, just to name a few.

An example of the common purpose among the rules is how Washington's Public Records Act, RCW §42.17.251, states, "The people of this state do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created." It is also common that there are points of contact within agencies for making requests and that the requests are in writing (sometimes including email or Web forms.) There is typically a wide range of media covered, such as the following list from North Carolina, "documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts or other documentary material, regardless of physical form or characteristic." (N.C.G.S. § 132-1)

Beyond the major similarities among the Federal FOIA and the State counterparts, there is variability in types of records covered, the exemptions, request procedures, timeframes, costs, and appeals procedures. Over time, original laws are modified and case law sets precedence for interpretations. The rules typically cover release of existing records, but not the records retention policies that may be established if there are records available. These variations contribute the differing impact on FOIA-type State regulations on TMC video recording procedures.

Best General Practice

Ask your State's office that handles FOIA requests how it processes release of video, including fees. If they do release video, ask them to check with their peers in other departments within the State.

The Federal FOIA includes nine exemptions (records that do not have to be released) and three exclusions (records whose existence isn't even covered by FOIA). The nine exemptions are national security interest, internal personnel rules of an agency, information prohibited from disclosure by other Federal laws, confidential or privileged trade secrets/commercial information/financial information, information that could invade personal privacy, certain law enforcement information, supervision of financial institutions, and geological information on wells. New Jersey's Open Public Records Act has 24 exemptions, some of which are analogous to Federal FOIA items, as well as more than a dozen exemptions established by executive orders.

The Minnesota Government Data Practices Act (Minnesota Statutes chapter 13) differentiates between traffic management video/still images and building security cameras. The former are public information and may be made available upon request, though release may be delayed until investigations are complete. Requests are processed by MnDOT traffic staff. Requests for security images undergo further evaluation under the Minnesota Government Data Practices Act and are only released if specific imagery is classified as public data.

While State public information law can be a major consideration for public release of recorded TMC video, it is not the only outlet for recorded video. As noted in the *Idaho Public Records Law Manual* quoting 4 Idaho Code § 9-343(3) (2011), "…nothing in the law limits the availability of documents and records for discovery in the normal course of judicial or administrative adjudicatory proceedings, subject to the law and rules of evidence and of discovery governing such proceedings." Also, some agencies make video available to the public outside of their jurisdictions' open records request process.

The most common exemption that applies to TMC video, whether technical FOIA requests or other public avenues, is while there is an active law enforcement investigation. During that time, the law enforcement agency has the video, but it cannot be released to other requestors. The TMC may store the video for them until the law enforcement agency concludes its investigation or the TMC may give the only copy to the law enforcement agency for them to release with the rest of the investigation report.

STATE PUBLIC RECORDS LAWS AND THE NECESSITY OF RECORDING

While FOIA-type laws dictate which records must be released to the public, it is typically State public records laws that dictate if material must be retained. Materials that are not kept do not need to be released. Public records laws could also be part of FOIA legislation. Records laws include both minimum amount of time that materials need to be kept and maximum times.

For example, under Wisconsin law, video on the automatic 72-hour recording loop is not considered a record that must be kept. Footage only becomes a record, and thus subject to open records rules, if it is selected to be kept beyond the 72 hours. In Washington, security video on buses is kept in on-board data storage until it is automatically overwritten. If the video is not downloaded from the on-board storage, it is not a record and does not need to be retained. However, if it is downloaded, it must be kept and released as public record. Washington's TMC has successfully asserted that video recorded for a study, such as a traffic study, is the equivalent to field photographs. Such foundational material is not subject to public records—only the resulting report is.

While not clearly spelled out in records retention laws, several agencies consulted for this report had spoken with their respective legal counsels and/or law enforcement agencies and did not find that there would be legal consequences for not recording or for not retaining recordings longer than a few days. As one agency who records most feeds for several days and makes them available to the public, the video is kept as a service, not as a right. The primary purpose of the camera feeds is traffic management by agency staff, law enforcement, and emergency responders. Those needs are met by the short-duration loop recording and keeping select clips longer. When discussing with their legal teams, the agencies noted the significant technical and financial burden of keeping large numbers of video feeds archived for more than a few days.

Agencies also noted that they included language in written policies for releasing or sharing video that did not guaranty availability of video, such as due to equipment failure. A legal expert also noted that it would be unlikely that any jurisdiction would have a legal basis for mandating recoding since traffic video is not a safety system.

VIDEO FOR USE AS EVIDENCE

From the perspective of a court of law, legacy video systems producing analog video were typically archived by a video tape, which was fairly straight forward to use as the process of recording was standardized by the playback mechanisms. Digital and IP-based video has complicated this procedure due to a lack of standardization of the technology for playback and storage. An IP-based video camera or encoder uses a compression algorithm to make the image smaller to transmit or store across sometimes limited communications mediums. This process by its nature introduces a degradation of the video that varies by device and potentially by use. How the video was encoded becomes a very important question with respect to video integrity, being able to certify that the video is complete and unaltered since acquisition, and authentication, being able to certify what is seen in the video is/was actually there. Artifacts could vary by compression type and be as simple as periods of no video or vehicles "skipping" in and out of the stream. By extension, if two agencies are recording a single stream, the archival process itself could also introduce additional distortions or artifacts such that if reviewed frame by frame the two stored video images are no longer the same. More simply put, the video encoding process itself could introduce distortions that could affect what image is being displayed which in turn could affect how a court would accept or use the video.

Unfortunately, since video technology varies and often changes more rapidly than laws, there does not seem to be uniformity. For example, there do not seem to be generally accepted compression or video formats for admissibility in courts or requirements for frame-by-frame authentication when live streams are recorded by multiple agencies. However, TMCs have still been successful defending the admissibility of video in court. The best general practices in the call-out box in this section reflect successful strategies.

Best General Practice

To support integrity of recordings for legal use:

- Discuss process with law enforcement stakeholders and your agency's legal department.
- Publicize and follow a standard process.
- Limit the number of individuals who process requests and have access to files.

There are two schools of thought on the TMC keeping an official copy of the video when releasing for legal use (when State law does not otherwise trump.) One is to keep a copy so that comparisons could be done or in case the requesting agency's copy is corrupted or lost. The other is to turn it over to the requesting agency and then delete it, thereby transferring the burden of maintaining it to the requesting agency.

Video management also offers options. For example, a digital watermark could be added. One agency adds a watermark for their own tracking purposes, rather than for legal proof. Some video management software packages have the capability to export clips in a proprietary format with a player as a strategy for limiting opportunities to tamper with the video. However, as one the agencies noted, it may become a burden to field complaints from the public when they have difficulty using the nonstandard player.

Although anecdotal, it seems that TMC video may not be scrutinized as heavily as video created by law enforcement departments or private companies. TMC video does not have the primary purpose of being evidence and the DOT typically does not have a stake in the outcome of a case involving their video, unlike security cameras used in casinos for instance. Still, if precedent is not clear within an agency already, it is recommended to discuss with law enforcement partners and agency legal counsel while also following a repeatable process and limiting individuals with access to the files.

PRIVACY

While TMCs generally record in public places, there seems to be a consensus that personally identifying information, such as license plates and faces, should not be shared with the public. For traffic management purposes, that level of detail is not needed and most often camera views and image quality preclude it anyway. For real-time video, agencies that cannot block video to the public may have policies not to zoom far enough to reveal the details. Also, if lower resolution video is shared real-time with the public, even significant zoom may not reveal that level of detail. However, there are instances where an agency may need to zoom in, such as to read hazardous material placards.

Typically, even when agencies can block real-time feeds to the public, the feeds are still recorded, which can bring privacy concerns. However, exemptions for privacy typically applicable to personal information kept for drivers through a Department of Motor Vehicles (DMV) may apply. Where an agency's video system includes security-only feeds, such as on door access, they are typically exempt since they show employees.

Perception of privacy is also a policy and operational concern outside of legal restrictions. Some agencies may choose not to record as a blanket policy to be responsible to local preferences.

LIABILITY

Variations in liability limits and laws affect an agency's risk. There are risks both for the size of possible award to plaintiffs and for the time required by TMC staff during legal discovery. The scale of the liability for award to plaintiffs can vary greatly if the State has a fixed cap, no cap, and/or joint and several liabilities. While agencies are not typically party to legal disputes related to video, when there is joint and several liabilities, particularly with no cap, there is more incentive for the "deep pocket" agency to be scrutinized for liability, even 1 percent. This is another matter in which there is great variability among jurisdictions so it would be necessary to inquire with the agency's legal counsel of applicable liability issues.

The following example of a State addressing liability for sharing real-time video is from the Tennessee DOT (TDOT):

> "3. LIABILITY AND INDEMNITY PROVISIONS:

> A. To the extent permitted by applicable law, 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 [closed-circuit television] 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.
>
> B. 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."

This excerpt is contained in their Access Agreement for Live Video and Information Sharing (both Responder and Private Entity version) which is in the appendix.

CHAPTER 7: PRACTICES FOR WRITTEN POLICIES AND AGREEMENTS

Agencies have varying levels of detail in written policies related to traffic cameras, if they have them at all. This chapter presents some of the highlights from policies used by agencies to give ideas of components to include when considering developing or revising policies.

PREVALENCE OF WRITTEN POLICIES

As shown in figure 11, for video sharing, there is nearly an even split between Transportation Management Centers (TMC) reporting having written policies and those that do not. There were also a sizeable number of respondents who responded as being unsure. For video recording, there is a higher skew to not having written policies.

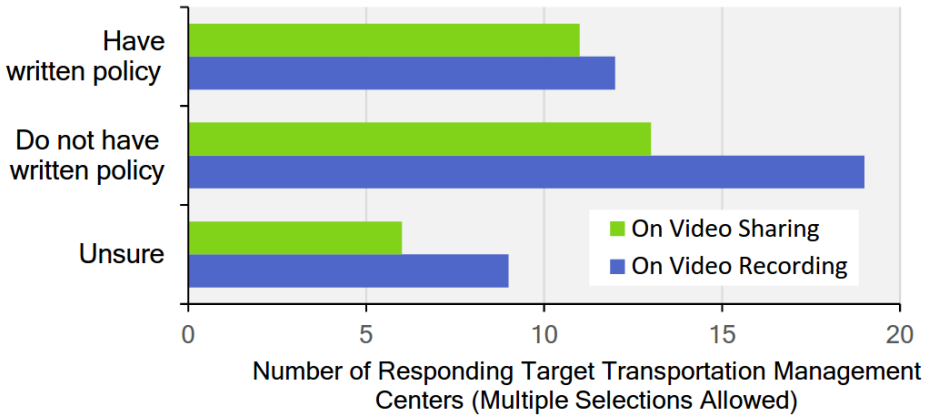


Figure 11: Chart. If existing written policies on video recording and video sharing.
(Source: Parsons Brinckerhoff)

Not having written policies allows for flexibility, but can occasionally lead to problems. For example, one agency without a written policy for sharing recorded video with local enforcement agencies recently faced a difficult situation. One of the Department of Transportation's (DOT) cameras caught the safe emergency landing of a small plane in a grass median. The DOT shared the clip with the local law enforcement department. Without permission of the recording/sharing agency, the law enforcement department posted the clip to its social media feed and it was picked up by mainstream media. While the clip was not damaging to any of the agencies or private parties involved, it revealed a difference in assumption of acceptable use as the DOT was not pleased.

OVERVIEW OF SAMPLE MATERIALS

The sample materials in the appendix cover a range of types of formats and include a variety of topic areas including video sharing, video recording, and cameras policies related to privacy. A listing is in table 6.

Table 6: List of written materials in the appendix.

Agency	Document Title	Content Topic Areas		
		Recording Video and Distributing It	**Sharing Real-Time Video**	**Camera Policies Related to Privacy**
Florida Department of Transportation (FDOT)	Closed-Circuit Televisions (CCTV) Agreement (02/12)	References that (FDOT) camera system does not record video	Agreement for sharing live video geared toward media is included	References sensitive images
Minnesota Department of Transportation (MnDOT)	Traffic Camera Use Office Practice (8/12/15)	Notes that recordings are public record even if live feed to public is cut	States that video is available to the public except under extenuating circumstances	Stresses traffic flow purpose; zooming out from identifying info
MnDOT	Traffic Camera Imagery Recording and Distribution (12/4/12)	Includes retention and distribution information	–	–
New York State Department of Transportation (NYSDOT)	Policy for the Design and Operation of CCTV in Advanced Traffic Management Systems (9/4/01)	States that recording is only permitted under limited situations	Notes that video is shared with the public, including through commercial means	Emphasizes not collecting or distributing personal identifier information
Niagara International Transportation Technology Coalition (NITTEC)	CCTV Policy (1/1/14)	Only on request of CCTV owner agency	Notes that images are shared through Web site	Discusses wide-angle view and not collecting personal identifier information
Oregon Department of Transportation	Use of CCTV Highway Cameras (4/16/14)	Notes that feeds are generally not recorded, except limited circumstance	Notes that images are shared with public	Lists operating guidelines to address privacy concerns
Tennessee Department of Transportation (TDOT)	"Access to Live Video Feeds and Information Sharing" (undated)	–	Policy is to make live feeds available to the public and to government agencies	–

Table 6: List of written materials in the appendix (continued).

Agency	Document Title	Content Topic Areas		
		Recording Video and Distributing It	**Sharing Real-Time Video**	**Camera Policies Related to Privacy**
TDOT	"Access Agreement for Live Video and Information Sharing—Private Entity Users" and corresponding Responder Entity Users version	States that TDOT will not record video except for training and that no recordings will be provided under this agreement	Includes details of TDOT and user responsibilities as well as liability and indemnity information	Notes that should not purposely broadcast zoom that shows individuals or license plates
Wisconsin Department of Transportation (WisDOT)	Is an undated template for a written agreement for using WisDOT video and/or data	Mentions that if the media shows recorded video, it must be labeled with date/time	Includes policies and guidelines for use and rebroadcast	Notes that feed can be cut

HIGHLIGHTS FROM VIDEO RECORDING AND DISTRIBUTING RECORDED VIDEO

As one agency that doesn't record video commented, there isn't a policy saying the agency doesn't record, everyone just knows it. Other agencies that don't record have notes to the effect in frequently asked questions (FAQ's) on their public Web sites. Some agencies mention the policy in related documents, such as how the Florida Department of Transportation's (FDOT) real-time video sharing agreement notes that they do not record video.

The New York State Department of Transportation (NYSDOT) has a detailed closed-circuit television (CCTV) policy document that includes the following section on recording:

1. "Except as provided for in this policy, CCTV data shall not be recorded and all data disseminated from CCTV systems shall be transferred in a real-time or limited-time-delay data feed. In all cases, recording shall only be done in a manner that protects the privacy of the public in accordance with this policy.
2. CCTV data shall only be recorded in response to a specific need where a review of the data would contribute to improving safety and/or future traffic operations procedures or system planning and performance including:

i. Review of a traffic operations or safety problem;
ii. Provision of a training review for future operator training;
iii. Research activities that will improve future technology or operations;
iv. Post-incident review of a particularly complex incident and emergency response for the purposes of improving operational procedures and response;
v. Demonstrating or testing equipment or system functions; or

vi. Collection of data for transportation planning management purposes where personal identifier information is subsequently removed from the data.

3. If a recording is made, it shall be retained in a specifically designated and secure location with access restricted by supervisory-level personnel.
4. CCTV system data which have been recorded shall be retained only for the minimum possible time after use of the archived data for its intended purpose in accordance with the applicable Department Records Retention Authorization."

The language above is from NYSDOT's Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems, September 4, 2001 which is in the appendix.

HIGHLIGHTS FROM SHARING REAL-TIME VIDEO

One relatively common feature of agreements for sharing video is that the Department of Transportation (DOT) is acknowledged. The Wisconsin Department of Transportation (WisDOT) has detailed language covering multiple formats, including social media:

Best General Practice

Written policies for video sharing provide an opportunity to require attributing the video feed to the DOT source, including the branding of the traveler information service if desired.

- "Any time WisDOT-provided video or data is broadcast via TV or other digital sources (including use on Web sites and social media applications), WisDOT should be acknowledged as the source either verbally, or by a graphic image of the WisDOT logo along with the picture.
- The WisDOT logo must appear on all broadcasted camera images. A broadcast-ready version of WisDOT's triskelion logo will be provided to you. Please ensure that the logo is visible and large enough to be clearly identifiable when using the camera images. Please also ensure that your corporate news channel banner does not conflict with the placement of the WisDOT logo."

The FDOT also influences what is around their video images, noting that "The Department requests that the Requestor provide a disclaimer of any Department endorsement of any advertising located near the video images." (Closed-Circuit Televisions (CCTV) Agreement, 2/12)

For entities to access FDOT's real-time video feeds, they install equipment at FDOT facilities to tie into the Department's video matrix switch. Their CCTV agreement contains many requirements for this connection, including that there is an initial $1,000 fee and an annual fee of $500 to cover coordination, security, and logistics.

NYSDOT's statements on video sharing emphasize the purpose of the sharing and notes:

> "The Department may also distribute CCTV data directly to the public via the Internet or other means for the purpose of providing traveler information. The Department shall take all reasonable efforts to ensure that any CCTV data disseminated in this manner shall not provide personal identifier information as previously defined in this policy. The sole purpose of providing such data shall be for the dissemination of traveler information to facilitate traffic management and the efficient balancing of transportation infrastructure demand and supply and all such uses and dissemination shall be consistent with statewide regulations, and this policy." (Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems, September 4, 2001)

The Tennessee Department of Transportation's (TDOT) written agreements for real-time video sharing leverage the desire of emergency response entities and private entities for the video into actions that support the DOT's traffic management goals. The access agreements for both emergency responders and for private entities include user responsibilities to:

- Notify TDOT of unexpected incidents, such as crashes, roadway debris, or traffic signal failures. For any incidents where TDOT or the Tennessee Highway Patrol are not already on scene, notification is to be made within 10 minutes of noticing the incident.
- Collaborate with TDOT for traffic management of planned events.

The access agreement for emergency responder entities further requires:

- Active participation in the National Traffic Incident Management (TIM) Responder Training Program, including that within one year of signing the agreement, any employee of the agency responding to the scene of the incident shall have attended on four-hour, in-person training session.
- Support for abiding by the safe and quick clearance approach.
- Active participation in TDOT's quarterly Regional TIM meetings, including providing the names of a primary individual and backup with authority to speak on behalf of the agency who will participate.

The access agreement for private entities invites them to:

- Participate in TDOT's quarterly Regional TIM.
- Attend TIM training.

Involving the media in TIM can be mutually beneficial during major incidents when news trucks are on scene, such as for agreeing on places to park and knowing who may be sharing information.

HIGHLIGHTS ON PRIVACY AND INTERACTION WITH LAW ENFORCEMENT

Oregon DOT's (ODOT) "Use of CCTV Highway Cameras" has a thorough list of operating guidelines geared to "respect for the privacy concerns of the public." It includes language on keeping cameras zoomed out when possible that is similar to many other policies. It also has

language related to overlap with law enforcement and also related to recording video. The complete list is:

1. "CCTV cameras will be set to view public right-of-way and zoomed out to view a sizable portion of the highway when not in use.
2. CCTV cameras will only be used to zoom in close enough to gather necessary information. Cameras will not be used to zoom in on individuals, especially where injuries are involved.
3. CCTV cameras will not be used to view the general public when not associated with an ODOT or law enforcement operation.
4. CCTV cameras will not be used to view any part of privately owned property; homes, businesses, etc.
5. CCTV cameras will not be used to zoom in on law enforcement activities occurring on or off the highways. Cameras may be used to aid law enforcement or provide additional eyes for safety. Cameras must be zoomed out or away immediately once requested assistance is rendered or sufficient officers to control the situation are on scene.
6. CCTV data will generally not be recorded or archived. Exceptions include cameras installed specifically for security and occasional recording for research or traffic analysis needs. Recorded images are considered public information and can be used as evidence."

Best General Practice

Leverage written agreements for real-time video streaming to emergency responders and the media for:

- Notifying lead agency of incidents, debris on roadways, signal outages, etc.
- Participating in TIM training.
- Support of safe quick-clearance.

The Niagara International Transportation Technology Coalition's (NITTEC) CCTV policy also includes the following language on when personal identifying video may be shared, "In the event of a public health danger or safety emergency, NITTEC may provide personal identifier information to such other public partner and/or entities as may be necessary to prevent, limit or mitigate such emergency."

The NYSDOT defines "Personal Identifier Information" as any data (including video) that:

1. "identifies an individual, drivers or passengers.
2. identifies license plate of vehicles.
3. identifies contents of the enclosed interior of passenger vehicles.
4. tracks the individual travel pattern of a specific vehicle."

HIGHLIGHTS ON LEGAL ISSUES

Legal issues vary by State so any included language should be vetted by the appropriate legal authorities. The following samples are provided to illustrate how some States have addressed issues.

The FDOT quotes statues Sections 119.07(2)(a) and 119.07(2)(c) as authorizing the DOT to remote electronic access and authorizing fees to be collected for the service.

The FDOT uses the following language on video availability and risks for using the video:

> "The Department does not guarantee the continuity of the video images, nor does it in any way warrant the accuracy or quality of the images provided.
>
> The risk of use of the images is the sole responsibility of Requestor and it agrees to be fully and solely responsible for and to indemnify, defend, and hold harmless, the Department, its agents, officers, and employees from any and all claims, damages, suits, actions or other proceedings for damages arising out of or in any way associated with the use of the video images by Requestor or in any way arising out of or associated with the placement or removal or failure to remove its equipment."

CHAPTER 8: CASE STUDIES

The case studies in this chapter will show a range of policy and procedure approaches that Transportation Management Centers (TMC) are using to maximize the potential benefits of recording and sharing video within their individual policy, institutional, technological, and fiscal constraints. The targeted agencies are listed in alphabetical order as the sections in this chapter.

IOWA DEPARTMENT OF TRANSPORTATION

Table 7: Transportation Management Center policies and procedures at the Iowa Department of Transportation.

Iowa Statewide Traffic Management Center (TMC)	• Over 300 cameras. • Records nearly all feeds for three days since September 2014. • Motor Vehicle Enforcement Officer has access to video management system.
Recording Practice	• The Executive Director of the Iowa Department of Transportation (DOT) led the decision to start recording all feeds to be used in training and after-action reports. Continuous recording started in 2014. • There were concerns about staff needed for releasing recorded video, especially since staffing was being reduced. Iowa DOT staff spoke with Minnesota DOT staff, who were also recording most of their cameras and fulfilling requests for video, and learned that it wasn't an overwhelming burden.
Releasing Recorded Video	• Both external and internal requests come through a Web link: http://www.iowadot.gov/511/trafficcameravideorequest.html (figure 12). • The page is NOT linked from elsewhere on Iowa DOT's Web site, but is given to law enforcement agencies. It does accept requests from individuals not associated with law enforcement agencies. • Reported a low burden responding to requests—few requests (a few each week; 90 percent from law enforcement) and adequate staff resources. • Currently, requests are mostly handled by the "Traveler Information Program Manager," but considering allowing the "Commercial Vehicle Enforcement Officer" to handle enforcement requests, especially so that law enforcement can obtain video faster. • When subpoenaed, they have been successful demonstrating integrity of video through a few strategies including limiting access to the video files to only a few people (major reason that TMC operators do not process video requests), sending them via secure File Transfer Protocol (FTP), and keeping a copy as an official record.
Sharing Real-time Images	• Iowa is the lead agency for the multistate Condition Acquisition and Reporting System (CARS) that includes video distribution through 511 and to over 100 other third-party entities. • Sharing images has been popular and well received.

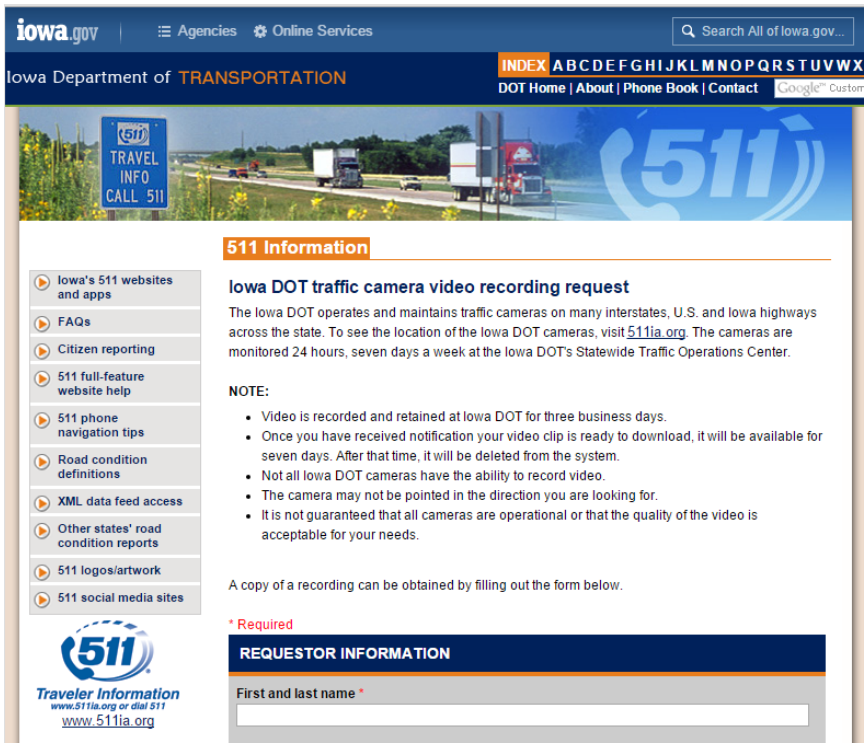


Figure 12: Screenshot. Iowa Department of Transportation Web site for requesting recorded video.
(Source: Iowa Department of Transportation)

MINNESOTA DEPARTMENT OF TRANSPORTATION

Table 8: Transportation Management Center policies and procedures at the Minnesota Department of Transportation.

Minnesota Regional Transportation Management Center (TMC)	• ~760 cameras. • Records nearly all feeds for 4 days.
Recording Practice	• Minnesota is believed to be the first State to record all feeds continuously. • Their recording program evolved as technologies changed, benefits of recording were recognized, needs changed, and opportunities for upgrading systems were seized. – Before 2002, Video home system (VHS) was manually activated for capturing incidents for training. – Between 2002 and 2007, several digital video recorders (DVR) were added to cover groups of cameras for specific needs (such as installation of new cable median barrier, change of a High-Occupancy Vehicle (HOV) lane to a High-Occupancy Toll (HOT) lane, and monitoring top crash locations). – In 2008, was able to shift to networked video recorder (NVR) "all camera" system based on the confluence of three factors: I-35 bridge collapse which highlighted the need for a redundant IP video backup to the existing analog video distribution network, significant server hardware was available at no cost from another Minnesota DOT (MnDOT) unit that didn't need it, and video management software was used for coordinating cameras for the 2008 Republican National Convention. – Some people within the agency had not been in favor of the expanded recording, but given the 2008 needs and opportunities, it was decided to try. It has continued since the value gained has been seen to outweigh the extra work distributing recorded video. • According to the "MnDOT Traffic Imagery Recording and Distribution" document dated 12/4/12, the retention time subject to change due to factors such as network health and compression efficiency, but requests should be received within two to four days so that video can be saved before automatic overwriting. • According to the same document, images archived by an operator are retained as follows: – For requests from a governmental agency for investigation, one year. – For requests from the media or the public, 90 days. – For research requests, may be deleted immediately following transfer to requestor. – For training or education, varies—can be deleted upon completion of training up through being kept indefinitely.

Table 8: Transportation Management Center policies and procedures at the Minnesota Department of Transportation (continued).

Recording Practice (continued)	• It is also effective to record the output of a dispatcher's monitor since it will capture moving incidents camera-to-camera such as pursuits and driving complaints. This captures what the dispatcher was viewing live which, along with 911 call audio and radio logs, provides a tidy and logical narrative for criminal court presentation. It is also significantly more efficient to save one video feed, instead of piecing together dozens of cameras over several minutes.
Releasing Recorded Video—Process and Burden	• Burden rates as low to medium for many requests, but adequate staff. Is about 1/5 Full-Time Equivalents (FTE) with an average of four requests per day, a number which has approximately doubled in the past five years. • Requests from the public and internal MnDOT requests can be via phone or email. Some requests come through the Minnesota Data Practices Office. The Minnesota State Patrol (MSP), approximately 50 percent of the requests, uses a written request form. The majority of MSP requests are for confirmed incidents, known to be captured on camera, like driving complaints (i.e., drunk drivers) and for non-valid drivers who have been cited and instructed to contact a valid driver, but then drive off after the Patrol leaves. The majority of public requests (including lawyers and insurance) are research requests to see if an incident was recorded, or if specific details are visible, which rarely is the case. • Video requests of one or two cameras, and up to about one hour, are archived as Microsoft audio video interface (AVI) file. Requests for multiple cameras and/or several hours, are fulfilled using the software's proprietary export process, requiring a viewer program. Proprietary exports must be distributed via a thumb drive or portable hard drive (for very large requests). Video clips requested by MSP are copied to a thumb drive on a weekly basis, the contents of which are then downloaded by a State Patrol dispatch supervisor to an MSP secure network location, available only to the MSP investigators who are offsite. The MSP investigators are then responsible for making copies for the requesting Trooper. Requests by non-State Patrol law enforcement, civilian, insurance, and lawyers are posted to a File Transfer Protocol (FTP) site and a link sent for them to download the file. MnDOT is currently investigating options for alternatives to FTP.

Table 8: Transportation Management Center policies and procedures at the Minnesota Department of Transportation (continued).

Releasing Recorded Video—Process and Burden (continued)	• Successful strategies for minimizing burden include: – Keep the process simple and scalable. Want to be able to be able to absolutely respond if a video exists of not within 20 seconds without referring to others to check. – Limit the number of people responding to archiving requests to prevent duplication and mislabeling. Preferably one person plus a backup. – Use electronic distribution (FTP or Dropbox) as much as possible. Avoid compact disc (CD)/digital video disc (DVD) duplication. Only use thumb drives or hard drives for very large requests. – Have a standard searchable file naming convention for recorded clips. Minnesota uses: [DATE] [TIME VIDEO STARTS] [APPROXIMATE LOCATION] [EVENT TYPE] [CASE NUMBER] [NAME OR BADGE OF REQUESTOR] [CAMERA NUMBER OR MONITOR OUTPUT].avi There is a space between each field. Date is preferably YR/MO/DA. Time is in 24-hour format. An example of event type is "DC"—driver complaint. Case number is omitted if not available. • Additional lessons learned: – Manage expectations for video quality and time to response (within business hours).
Releasing Recorded Video—Legal and Evidence Issues	• Meet with law enforcement investigators to discuss their policies/practices of releasing their squad car video and discuss what could be applied to Transportation Management Center (TMC video. • Clearly define with law enforcement how video will be released. Preferably, make one copy, give it to the lead agency, and make them responsible for further release (such as to the prosecutors, defense, media, etc.) They could release the video as part of the record of the investigation. • Have a standard practice for logging video evidence and making it available to support chain of custody. • Having a manager, or at least supervisor, handle archiving also has the benefit of limiting who would be called by a subpoena to appear in court. • There haven't been problems with the video not being encrypted or time stamped (as it is in casinos.) It may help that the Department of Transportation (DOT) is seen as neutral in most cases, as opposed to casinos which both manage the video and have an interest in the case. • Privacy hasn't been a major concern since roadways are public space and there is little expectation of privacy. Some exceptions exist, such as identifying individuals or viewing homes. Note that public information availability statues protect students in a school setting which includes school buses.

Table 8: Transportation Management Center policies and procedures at the Minnesota Department of Transportation (continued).

Sharing Real-Time Images	• Streaming video is shared with other roadway agencies, law enforcement/emergency responders, television media, and some professional traffic reporting companies. • Due to bandwidth, streaming to 511 is limited. Instead, stills are posted.
Camera Use Policy	• Recognizing that camera video is typically available real-time and can be requested, the "Traffic Cameras Use Office Practice" dated 8/12/15 requires that all users of the camera system position the cameras to traffic flow. Even when viewing an incident, the camera MUST be zoomed far enough out such that people cannot be identified by their faces. • There is an option in the Active Traffic Management System (ATMS) software (IRIS) to "un-publish" individual cameras so they are blocked from real-time viewing outside the TMC. This option is only available to TMC staff. Cameras are only to be un-published under very limited circumstances such as fatal or potentially fatal incidents when the camera cannot be repositioned away from personally identifiable vehicles or individuals, national security events (like Presidential motorcades) or when a camera is stuck in an inappropriate view, such as a house. The feature was added in 2008.

NEW JERSEY DEPARTMENT OF TRANSPORTATION

Table 9: Transportation Management Center policies and procedures at the New Jersey Department of Transportation.

New Jersey State Transportation Management Center (STMC)	• More than 400 cameras. • Records most feeds continuously.
Recording Practice	• Feeds are retained for a minimum of seven days before being automatically overwritten. • New Jersey Department of Transportation (NJDOT) has trailer-mounted cameras and a vehicle-mounted camera that has been used from an Incident Management Response Team vehicle during major special events.
Release of Recorded Video	• Information for the public to request video is posted at http://www.state.nj.us/transportation/business/videolog/. • There is a PDF form that must be emailed within seven days of incident. • The requests do not go through the typical NJDOT Open Public Records Act processing agency, the Official Custodian of Records within the Office of Inspector General. Rather, they are routed to the State Transportation Management Center (STMC). • Many requests, particularly from the public, are well beyond the published availability or have referenced cameras that are actually video detection cameras. • The STMC manager typically processes requests, both for law enforcement partners and from the public. • Initially, the agency released clips in the agency's video management system's proprietary format with the copy of the video management' system's video player. However, many recipients had difficulty accessing the video. • Currently, the agency converts the video to Microsoft's Advanced Systems Format (ASF) prior to release. • For the public, fees can be charged: $100 first three hours and $50 per hour thereafter plus any postage. Fees collected go into a general fund for NJDOT activities, not to the STMC budget.
Highlighted Benefits of Releasing Recorded Video	• Sharing video with local enforcement agencies has been very beneficial for developing rapport that strengthens Traffic Incident Management (TIM) activities. • Recorded video from portable cameras in work zones can be used to check if lanes are opened and closed within allowable schedules.
Sharing Real-Time Images	• Streaming video is available to the public via 511NJ. • New York-New Jersey-Connecticut area agencies also share cameras with each other through a login-based system. • Special events and major construction projects have been the catalysts for extra cameras and increased sharing among agencies.

REGIONAL TRANSPORTATION COMMISSION OF SOUTHERN NEVADA

Table 10: Transportation Management Center policies and procedures at the Regional Transportation Commission (RTC) of Southern Nevada.

RTC of Southern Nevada	• Approximately 500 cameras. • Never records video. • Does collect screen shots for performance management and studies.
Recording Practice	• At one time, video was recorded for seven days, but following a negative experience with an incident, it was decided not to record. • Recording streaming video is not considered necessary for traffic management functions.
Snapshots	• Their central software allows technicians to right click on the map to create an incident record (figure 13). • One of the tabs allows users to populate a 3x3 grid with nearby cameras. Using a custom script, a composite of the images is recorded every 15 seconds for the duration of the incident (figure 14). • The images can be reviewed later to collect key incident clearance events (figure 15.) The images also reveal length and dissipation of queues.
Sharing Real-time Images	• Streaming video is available through the agency's Web site and it is provided to the media. • The agency's Web site includes a form to take user questions and reports of camera views that are unavailable. • The main value to the travelers is considered to be through the media since there is greater exposure. It also shows the public that the cameras are being used to provide value.

Figure 13: Screenshot. Snapshot of central software used by the Regional Transportation Commission (RTC) of Southern Nevada.
(Source: RTC of Southern Nevada)

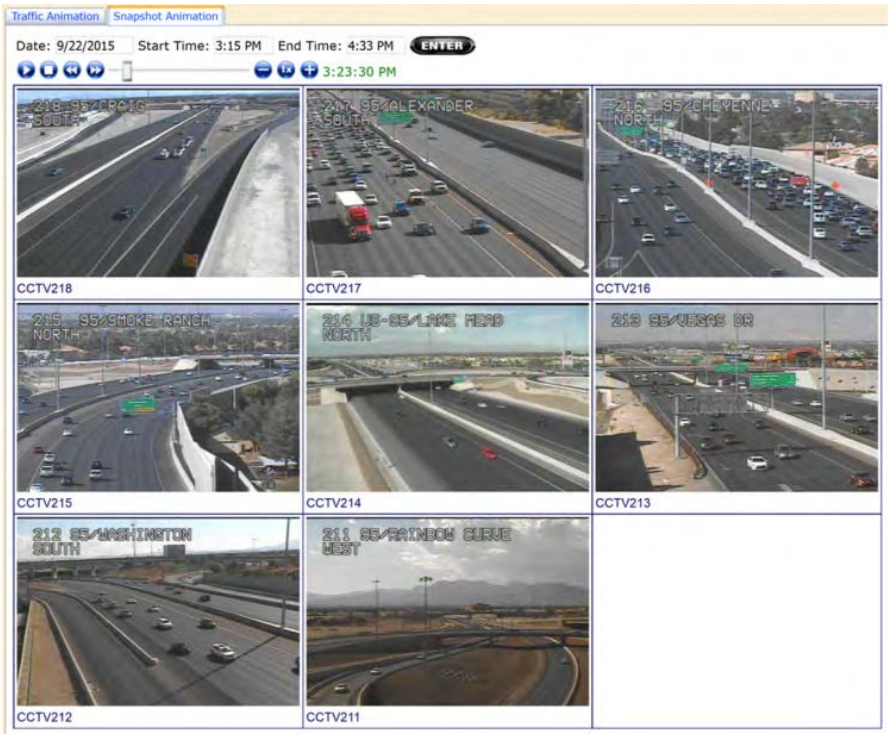


Figure 14: Screenshot. Snapshot of image recording feature during incidents within the central software used by the Regional Transportation Commission (RTC) of Southern Nevada.
(Source: RTC of Southern Nevada)

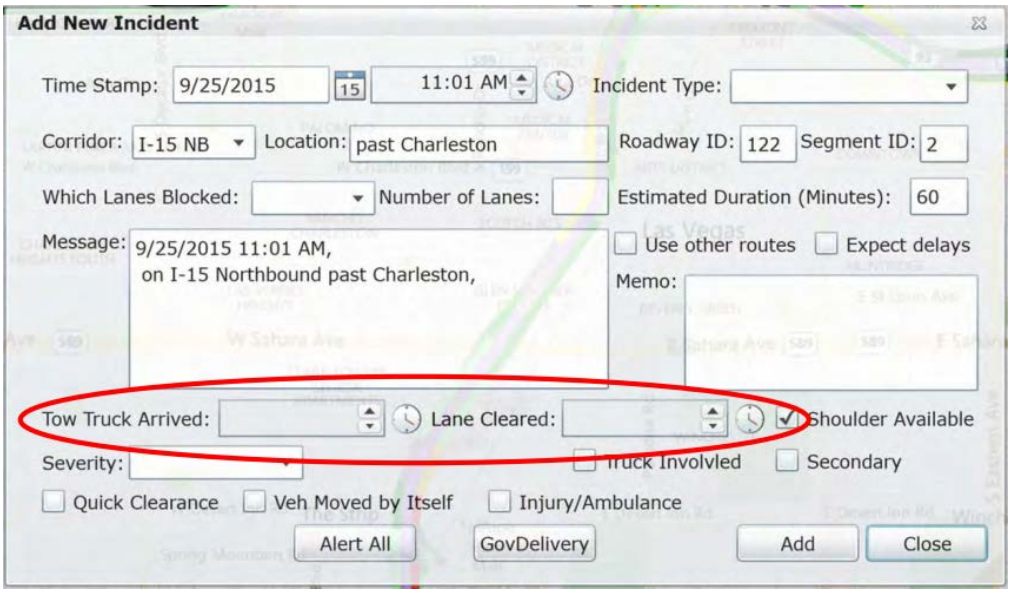


Figure 15: Screenshot. Snapshot of information collected from images within the central software used by the Regional Transportation Commission (RTC) of Southern Nevada. (Source: RTC of Southern Nevada)

TENNESSEE DEPARTMENT OF TRANSPORTATION

Table 11: Transportation Management Center policies and procedures at the Tennessee Department of Transportation.

Tennessee Department of Transportation (including their four regional TMCs)	• ~500 cameras. • Only record for training purposes. • Leverages agreement to share video for enhanced notification of incidents to Tennessee Department of Transportation (TDOT) and also for enhanced Traffic Incident Management (TIM) participation.
Recording Practice	• TDOT focuses on the use of real-time video for traffic management, limiting recording to training purposes. Also: – Only one stream at a time can be recorded. – Lack of storage space for extensive recording. – There is a lack of staff resources to handle requests for extensive archived video.
Releasing Live Video	• One Department of Transportation's (DOT) information technology (IT) department determined that the legacy access provided by the media for streaming video was not secure enough. That need, along with the needs to provide access to local agencies inexpensively and to provide easy video access for senior team to view ongoing events, prompted procurement of a new software solution to handle video sharing. It includes modules for media access, emergency responder access, and an executive view portal. • Video is streamed to a mobile Web site, as shown in figure 16 from a TDOT promotional video for their SmartWay traveler information service (video available at https://smartway.tn.gov/#traffic-app).

Table 11: Transportation Management Center policies and procedures at the Tennessee Department of Transportation (continued).

Releasing Live Video—Access Agreements	• The access agreements for both emergency responders and for private entities include user responsibilities to: – Notify TDOT of unexpected incidents, such as crashes, roadway debris, or traffic signal failures. For any incidents were TDOT or the Tennessee Highway Patrol are not already on scene, notification is to be made within 10 minutes of noticing the incident. – Collaborate with TDOT for traffic management of planned events. • The access agreement for emergency responder entities further requires: – Active participation in the National TIM Responder Training Program, including that within one year of signing the agreement, any employee of the agency responding to the scene of the incident shall have attended a 4-hour, in-person training session. – Support for abiding by the safe and quick clearance approach. – Active participation in TDOT's quarterly Regional Traffic Incident Management meetings, including providing the names of a primary individual and backup with authority to speak on behalf of the agency who will participate. • The access agreement for private entities invites them to – Participate in TDOT's quarterly Regional Traffic Incident Management. – Attend Traffic Incident Management training. • Involving the media in TIM can be mutually beneficial during major incidents when news trucks are on scene, such as for agreeing on places to park and knowing who may be sharing information.

Figure 16: Photo. Screen capture of the Tennessee Department of Transportation's SmartWay traveler information service.
(Source: https://smartway.tn.gov/)

WASHINGTON STATE DEPARTMENT OF TRANSPORTATION

Table 12: Transportation Management Center policies and procedures at the Washington State Department of Transportation.

Northwest Region Transportation Management Center (TMC)	• ~700 cameras (adding 500 more, including tunnel safety cameras, in near future). • Only record under limited situations.
Recording Practice	• The Washington State Department of Transportation (WSDOT) has a long-standing practice of only recording for specific limited purposes, such as training, data collection/observation, special events, and research. • They stress aligning use of video to the agency's mission. • Recordings are typically kept for less than a week, though recordings that are used as visual support to a study may be kept as long as needed. • Recordings may be deleted after sharing with the requesting entity. • For security cameras, which are on the same network as traffic management cameras, the practice is to record on a three-day loop so that investigations can be made of things that happened over the weekend.
Releasing Recorded Video	• Recordings are typically considered "raw data," much like field photographs, so are not subject to retention and release like reports are. • The public can request recordings of video under the Washington State Public Records Act through the WSDOT Records and Information Services office in Olympia. The request would then be routed to the appropriate Transportation Management Center (TMC) based on location for checking if a recording exists. By law, a response is required within five business days containing, the record requested, an acknowledgment of the request with an estimate of time to process, or a denial. • However, requests are almost certainly futile since so little video is kept or considered a record.
Sharing Real-Time Images	• The WSDOT Web site shows still images updated every two minutes. • Video is also shared with other roadway agencies, law enforcement/emergency responders, the media, and third parties. • More than a decade ago, WSDOT had a formal agreement for sharing video including a hold harmless clause, but video is now so widely distributed it was deemed not necessary. • WSDOT developed a module for their freeway management software in-house that allows selective cutting of feeds to various users. • Entities that receive shared video may record video per their own record-keeping policies.

WISCONSIN DEPARTMENT OF TRANSPORTATION

Table 13: Transportation Management Center policies and procedures at the Wisconsin Department of Transportation.

Statewide Traffic Operations Center (STOC)	• ~400 cameras. • Records nearly all feeds for at least 72 hours. • Statewide 24/7 coverage since 2007.
Recording Practice	• When STOC was created in 2007, video management systems were put into place that enabled the continuous recording of all feeds. Current practice is: – Nearly all cameras recorded for a minimum of 72 hours. The agency does not feel a need for a longer minimum time. – If a clip is tagged for saving, it will be saved for a maximum of 120 days. • Prior to that, recording was sporadic using video cassette recorders (VCR) after an incident was detected. • The Wisconsin Department of Transportation (WisDOT) decided to record all of the feeds because it recognized the value in being able to see and understand the beginning of the incident. The technology was available at the time of the investment in creating the STOC to enable the change.
Benefits of Camera Images in Traffic Incident Management (TIM)	• From WisDOT's "CCTV's [Closed-Circuit Televisions] Role in WisDOT's TIM [Traffic Incident Management] Success" CCTV/TIM webinar, by Anne Rashadi, P.E. WisDOT Bureau of Traffic Operations and Daniel Graff, WisDOT Office of General Counsel, November 21, 2013 (figures 17 through 19).
Release of Recorded Video	• Under Wisconsin law, video is a "record" and as such is subject to open records and video selected to be kept beyond the automatic 72 hours is subject to records retention requirements. Video will be released unless it would violate a specific set of conditions, though it would not be available until after law enforcement have an active investigation. • The Archive Video Administrator spends an average of six to eight hours per week processing zero to four requests per day each taking 15 to 60 minutes. The agency considers this a low burden since while there are many requests, there are adequate staff resources. • There is no cost to requestors. • Video is typically distributed on a digital video disc (DVD), but other media can be used for larger requests. • To limit requests for areas without camera coverage, the agency suggests that requestors check 511 for camera locations. • In-house information technology (IT) staff wrote a helpful program to tracks requests for video.

Table 13: Transportation Management Center policies and procedures at the Wisconsin Department of Transportation (continued).

Sharing Real-Time Images	• The written policy (in the appendix) for using WisDOT video and/or data includes that: – WisDOT should be acknowledged as the source through a logo or verbally, including on social media. – The video and data are intended for traveler information purposes only so should be the most recent versions. Any noncurrent data must be labeled with the date and time of recording. • The vast majority of camera images are available online and to media, but there are few available at the STOC and used for security that are not shared.

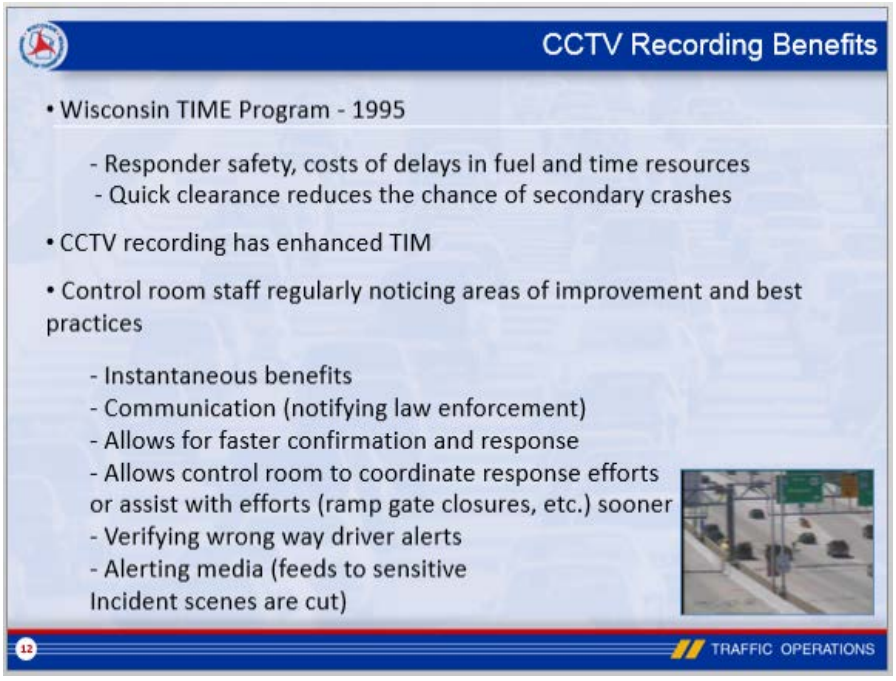


Figure 17: Screenshot. Presentation slide detailing the benefits of closed-circuit television recording for the Wisconsin Department of Transportation (WisDOT), part 1. (Source: WisDOT)

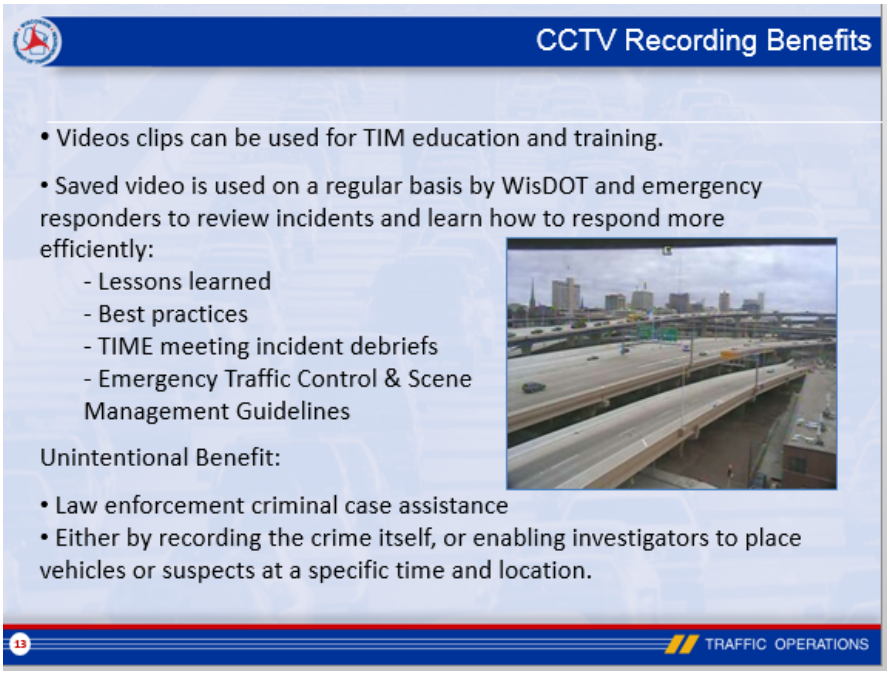


Figure 18: Presentation slide detailing the benefits of closed-circuit television recording for the Wisconsin Department of Transportation (WisDOT), part 2.
(Source: WisDOT)

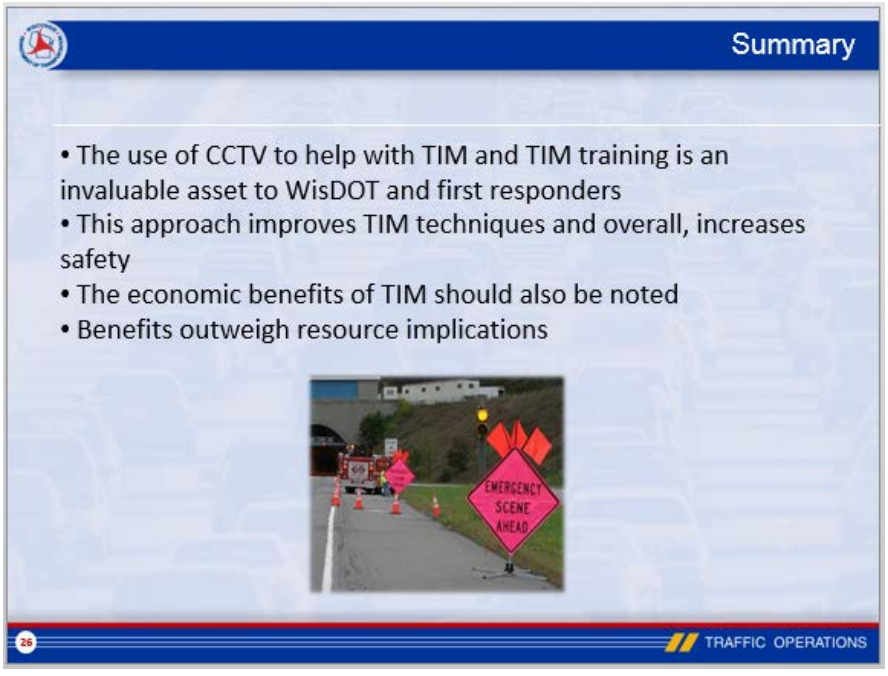


Figure 19: Presentation slide detailing the benefits of closed-circuit television recording for the Wisconsin Department of Transportation (WisDOT), part 3.
(Source: WisDOT)

APPENDIX. SAMPLE AGREEMENTS AND POLICIES

STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION

CLOSED CIRCUIT TELEVISION (CCTV) AGREEMENT

THIS AGREEMENT, made and entered into this_____day of_____by and between the Florida Department of Transportation, an agency of the State of Florida, hereinafter called the "Department" whose office address is 605 Suwannee Street, MS #90, Tallahassee, Florida 32399-0450 and_____, hereinafter called the "Requestor", whose office address is_____.

1. The Department operates computerized motorist information systems which monitor traffic conditions on certain portions of the State Transportation System.

2. The system provides a "live" video image. The images are not recorded.

3. Requestor has asked for remote electronic access to the video images created by the system operated in the _____ area.

4. Pursuant to Section 119.07(2)(a), Florida Statutes, the Department is authorized to provide access to public records by remote electronic means, provided exempt or confidential information is not disclosed.

5. Pursuant to Section 119.07(2)(c), Florida Statutes, the Department is authorized to charge a fee for remote electronic access including the direct and indirect costs of providing such access.

6. The Department will provide to Requestor the requested "live" video images generated by the Department's Closed-Circuit Television (CCTV) cameras used for monitoring traffic conditions in the _____ area, as available. The video images provided shall be those currently available to the Department control room operators from the images on the traffic surveillance monitors within the control room. This Agreement is non-exclusive and nothing herein shall be deemed to limit the ability of the Department to provide the video images referenced herein to other parties.

7. In order to receive the signal Requestor shall provide, operate, and maintain, at its own risk and expense, all equipment, hardware, or software (including, but not limited to, the interface equipment to tie into the Department's video matrix switcher). The Department assumes no responsibility for any equipment or property placed in the Regional Traffic Management Center(s) (RTMC) or another Department approved facility and Requestor hereby expressly relieves and discharges Department from any and all liability for any loss, injury, or damage to persons and property that may be sustained by reason of the use or occupancy of the Department's RTMC(s) or Department approved facility. Requestor agrees to immediately move or relocate, at its sole expense, any or all of the equipment, hardware, or software at the request of the Department. Requestor shall provide a fully trained contact person who is solely responsible for the operation and maintenance of Requestor's equipment and all activities associated with this Agreement. The Department shall have no responsibility to provide any training or supervision of Requestor's contact person associated with this Agreement other than to allow the contact person to attend all briefings and/or training sessions provided by the Department which relate to the equipment, hardware, or software. The contact person shall have access to Requestor's equipment, hardware, and software between 8:00 a.m. and 5:00 p.m., Monday through Friday for purposes of maintenance, repair, replacement, or upgrading of said property of Requestor. When possible, such access will be arranged in advance. A Department escort may be required during these hours in accordance with security measures at these facilities.

8. Requestor agrees that it will not install or operate any equipment, hardware or software that may interfere with the Department's CCTV traffic surveillance camera systems, any Department communications equipment or other Department electronic systems. In the event any such interference occurs, Requestor shall immediately remedy all problems caused by such interference. Requestor further authorizes the Department to disconnect or deactivate any equipment, hardware or software causing such interference and waives any claim it might otherwise assert as a result of such disconnection or deactivation.

9. The Department requests that the Requestor give appropriate on-screen, on-air, online, and in-print attribution to the Department for use of the video images.

10. The Department requests that the Requestor bear in mind the content of the images when broadcasting. The video feed may contain sensitive images that can be disturbing or offensive to some viewers, potentially including images of persons or vehicles involved in fatal accidents; law enforcement stops or pursuits of vehicles; identifiable images of the general public or license plates of vehicles; or images of catastrophic events.

Figure 20: Sample scan. Closed Circuit Television (CCTV) Agreement (page 1 of 2). (Source: Florida Department of Transportation)

11. The Department requests that the Requestor provide a disclaimer of any Department endorsement of any advertising located near the video images.

12. The Department does not guarantee the continuity of the video images, nor does it in any way warrant the accuracy or quality of the images provided.

13. The risk of use of the images is the sole responsibility of Requestor and it agrees to be fully and solely responsible for and to indemnify, defend, and hold harmless, the Department, its agents, officers, and employees from any and all claims, damages, suits, actions or other proceedings for damages arising out of or in any way associated with the use of the video images by Requestor or in any way arising out of or associated with the placement or removal or failure to remove its equipment.

14. Vendor/Contractor:

    (1) shall utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the Vendor/Contractor during the term of the contract; and

    (2) shall expressly require any subcontractors performing work or providing services pursuant to state contract to likewise utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the contract term.

    (See *Form #375-040-68, E-Verify*)

15. If Requestor wishes to stop receiving the video images, Requestor shall advise the Department in writing and shall remove all of its equipment, hardware, and software within thirty (30) days. If Requestor fails to remove its equipment, hardware, or software within thirty (30) days the Department may remove and dispose of any equipment, hardware, or software, without any liability to the Requestor.

16. The video images will be provided to the Requestor on an ongoing basis at no charge. However, to cover the cost of security and logistics coordination during the initial video connection phase, a non-refundable One Thousand dollar ($1,000) fee will be required at each RTMC or approved Department facility, where Requestor installs equipment. Requestor will pay an annual fee of Five Hundred dollars ($500) at each RTMC or approved Department facility where Requestor has installed equipment, covering the cost of security and logistics coordination for providing access to Requestor's equipment in order to perform routine equipment maintenance. The Requestor will be invoiced for the routine equipment maintenance access fees annually on the date of the original agreement. The Department may adjust the annual routine equipment maintenance fee for a subsequent year upon providing written notification to Requestor of the change. Any subsequent major equipment upgrades may require an additional One Thousand dollar ($1,000) fee at each RTMC or Department approved facility, where Requestor has installed equipment. In the event the Department determines that Requestor caused damage to Department equipment or facilities, Requestor shall reimburse the Department for all damages it caused within 30 days of notice from the Department.

IN WITNESS WHEREOF, the parties to this Agreement have signed this Agreement as of the date written below:

REQUESTOR	**STATE of FLORIDA** **DEPARTMENT of TRANSPORTATION**
By: _____ (NAME PRINTED)	By: _____ (NAME PRINTED)
_____ (TITLE)	_____ (Traffic Operations-Title)
Date: _____	Date: _____
	Legal Review: _____ Central Office

Figure 21: Sample scan. Closed Circuit Television (CCTV) Agreement (page 2 of 2). (Source: Florida Department of Transportation)

Camera Use

Traffic Camera Use Office Practice August 12th 2015

All users of the camera system, including agency partners, are required to follow this practice.

The cameras are for traffic management purposes. This includes monitoring traffic flow, verifying proper TMC equipment function (DMS, ILCS, and ramp meters), and detecting, assessing, and monitoring incidents on the roadway. Viewing incidents not on the roadway should be limited to only those with a reasonable chance they may cause an impact to roadway traffic flow. When not monitoring an incident the cameras shall be pointed at the roadway, fully zoomed out. When monitoring an incident, the camera should be kept in a position that still allows view of the larger area while balancing the needs for monitoring the incident.

The traffic camera video is available at all times live to the public on the Internet and to the local TV stations. Camera images are public data and cannot be withheld except in extraordinary circumstances. The public nature of the cameras must be kept in mind at all times, especially regarding zooming in on incident details and personally identifying information.

All users shall **continually** check to make sure camera views are appropriate and make corrections as needed. Freeway Operations staff should check all cameras at beginning and ending of shift, as well as a minimum of once an hour per person.

Position

Standard camera position is zoomed out, with a maximum view of the freeway mainline and a minimal amount of horizon across the top. Arterial cameras should be kept on the roadway, turned in a direction that allows a view of at least one direction of queued traffic, unless Signals Operations has requested a specific intersection view.

It is important that all cameras are positioned to view traffic flow. Even when watching an incident, the camera MUST be zoomed out far enough so that you cannot identify people (i.e. by their face).

Inappropriate Camera Use

If a camera is being used inappropriately, personnel should make one attempt to correct the issue. If it continues, notify the Freeway Operations Supervisor by email with the date, time and camera number and a brief description of the incident. Continual inappropriate usage may result in the loss of camera control privileges.

Blocking Video Feed / Un-publishing a Camera

Cameras shall be kept available (published) as often as possible. However, there are rare incidents when a camera may be blocked from public view and available only for internal purposes. Un-publishing a camera is at the discretion of Freeway Operations staff. Un-publishing a camera does not affect camera recording as recorded data is still public and is required to be turned over upon request. Public safety partners outside the RTMC (like ambulance and fire dispatch) also lose their camera view when the feed is blocked. Cameras shall be returned to public view (published) at the earliest point practical.

Figure 22: Sample scan. Camera Use Policies (page 1 of 2).
(Source: Minnesota Department of Transportation)

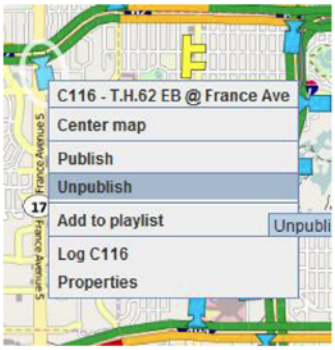
The events in which un-publishing a camera is necessary include:

- A fatality or serious injury incident where the body, or involved vehicles, is personally identifiable and the camera view cannot be repositioned
- An incident with a reasonable chance of becoming a fatality (example: jumper, felony stop, suicidal person) and the camera view is needed for managing the incident
- At the request of Secret Service for the President's or Vice President's motorcade
- Camera is stuck in a position showing an inappropriate view (example: stuck pointed at a house)

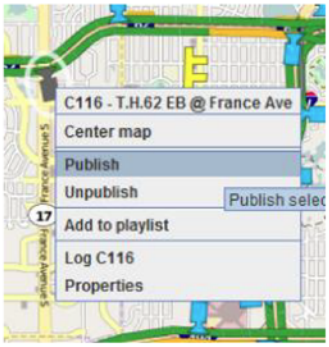
How to Un-publish / Publish a Camera

Right-click on the blue camera icon on the map in IRIS and choose "Unpublish." When the camera is un-published in IRIS, that camera will turn to a black camera symbol. To publish the camera, right click on the black camera symbol in IRIS and choose "Publish."

Published Camera



Unpublished Camera



Other Agency Use

Agency partners with full camera control include:

- Minnesota State Patrol (RTMC floor)
- MnDOT Maintenance (RTMC floor)
- MnDOT Traffic Engineering/Signals (RTMC floor)
- KBEM broadcaster (RTMC floor)
- MnDOT RITSM and Design/Integration (RTMC LL and 1st floor)

Other Agencies with access to live analog video but no control include:

- Metro Transit
- Minneapolis TMC and Hennepin County traffic signals
- TV Stations (WCCO, KARE, KMSP, KSTP)
- Ramsey County 911 Dispatch

Agencies with access to digital streaming video via Milestone or IRIS include:

- Professional traffic reporters
- Several local 911 dispatch centers

Figure 23: Sample scan. Camera Use Policies (page 2 of 2).
(Source: Minnesota Department of Transportation)

12/4/2012

MnDOT Traffic Camera Imagery Recording & Distribution

Overview

MnDOT owns, operates, and is responsible for a large network of traffic management closed circuit television cameras (CCTV) on highways and freeways in the Minneapolis/St Paul Metropolitan area and in several outstate locations.

MnDOT may record video or still images transmitted from the cameras. Under the Minnesota Government Data Practices Act (Minnesota Statutes Chapter 13) these images are public information and may be made available upon request. In cases where the images are part of an active investigation, public distribution may be delayed until its release is authorized by the authority performing the investigation.

MnDOT may charge a reasonable amount and require pre-payment for searching and retrieving, copying or transferring the imagery, and for shipping and other costs as permitted by the Minnesota Government Data Practices Act. MnDOT may require the requester to provide a data storage device sufficient for transferring the data. See Requesting Imagery and Distribution section for further guidance.

These guidelines refer to imagery generated from public access highway and freeway traffic monitoring, and do not apply to security imagery generated from internal and external building security cameras for the purpose of safeguarding MnDOT's employees, campus areas and infrastructure. Requests for security imagery will be evaluated under the Minnesota Government Data Practices Act and imagery classified as public data will be provided in a reasonable time frame.

Retention

Retention time of images is subject to change due to several factors including, but not limited to; system or network health, compression efficiency, changes in technology, or changes to MnDOT's needs. Requests for imagery must be received before automatic overwriting (usually within 2-4 days after an incident) or the imagery will be lost through the automatic overwriting process.

Usual Imagery Retention

- Imagery automatically captured and temporarily stored by the system without operator intervention – 2 to 4 days.
- Imagery archived by an operator at the request of a governmental agency for investigation – 1 year.
- Imagery archived by an operator at the request of the media or the public – 90 days.
- Imagery archived by an operator for a research request – may be deleted immediately following its transferal to the requester.
- Imagery archived by an operator and identified as valuable for training or education may be stored indefinitely or deleted upon the conclusion of training.

Figure 24: Sample scan. Minnesota Department of Transportation (MnDOT) Traffic Camera Imagery Recording and Distribution Policies (page 1 of 2).
(Source: Minnesota Department of Transportation)

12/4/2012

Requesting Imagery and Distribution

Requests for MnDOT traffic camera imagery should be directed to the appropriate office, as listed below. For areas not listed, contact the MnDOT district engineer for that area.

- Duluth Area – MnDOT District 1 – 218-725-2700
- St Cloud area – MnDOT District 3 – 320-223-6540
- Metropolitan Area – MnDOT Freeway Operations – 651-234-7500
- Rochester Area – MnDOT District 6 – 507-286-7500

The requester is required to provide the location, date, and time or time range for the imagery desired. Distribution via electronic mail or FTP is the preferred method. Requests requiring CD or data DVD transfer may incur additional expenses for media and shipping. Requests for data beyond the capacity of a single-layer data DVD or the FTP site may require the requester to provide an appropriate data transfer and storage device, such as an external flash or hard drive, and the requestor is responsible for all shipping charges, including return shipping.

MnDOT will make a reasonable attempt to provide the imagery data in a non-proprietary format, viewable on a PC. The Department will not provide conversion services (such as digital to analog or AVI to MPEG) and is not responsible for end-user data incompatibility.

MnDOT does not guaranty that the imagery recording system will always exist as a whole, that it will be uninterrupted or error-free, that individual cameras will be recorded, or that requests for imagery will be responded to prior to the end of the retention period. Responsible staff will make a reasonable attempt to recover imagery requested within normal hours of business operation (8-4:30, M-F). MnDOT is not responsible for imagery that is not exported prior to the automatic deletion period, or imagery that is lost or deleted due to operator error or mechanical failure. Requests for large amounts of data may be denied if providing the data would overload storage capacity or otherwise damage the technical or mechanical infrastructure.

MnDOT is currently seeking confirmation of this retention policy through appropriate channels. Any required changes will be incorporated in to future policy revisions.

Figure 25: Sample scan. Minnesota Department of Transportation (MnDOT) Traffic Camera Imagery Recording and Distribution Policies (page 2 of 2).
(Source: Minnesota Department of Transportation)

Traffic Engineering and Highway Safety Division

Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems

September 4, 2001

I. Introduction.

The New York State Department of Transportation ("Department") has and is installing closed-circuit television systems ("CCTV systems") along certain state roadways as part of its Intelligent Transportation Systems ("ITS") program. The ITS program includes the use of technology to address transportation needs. The CCTV system is an element of Advanced Traffic Management Systems ("ATM Systems") that allow the Department to manage its roadway system in a manner that maximizes the efficiency of the existing facilities. This is critically important in congested urban areas where it may not be possible or desirable to add roadway capacity.

ATM Systems use technologies such as CCTV systems, traffic detectors and electronic message signs to monitor and collect information on traffic conditions, manage traffic, quickly detect incidents, dispatch the proper response and provide motorists advance notice of congestion, reducing the possibility of secondary accidents and allowing motorists to consider alternate routes, modes or travel times. These systems are run from Transportation Management Centers ("TMC") where managers and operators analyze the input from the field devices, manage traffic via the ATM system elements and coordinate the fastest and best response to the incident.

The use of CCTV cameras are an integral part of these systems in New York State as well as throughout the country. The CCTV systems are a valuable source of data, specifically, traffic conditions, and/or traveler information to be provided to the public. Traffic or traveler information is provided to the traveling public to alert them to roadway conditions, incidents ahead or on adjacent roadways, anticipated travel times, congestion, detour recommendations, and advance notice of future roadway condition changes anticipated as a result of special events or roadway construction activities. Accordingly, the Department shares the data with media and traveler information service providers for the purpose of distributing information to the widest audience possible. In this context, CCTV systems are data/information-collecting tools. They must be utilized in a consistent manner that strives to uphold the public's expectation of privacy, while serving their function as a traffic management and traveler information tool.

II. Applicability.

This policy establishes the manner in which the public's reasonable expectation of privacy is

Figure 26: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 1 of 11).
(Source: New York State Department of Transportation)

protected where the Department deploys Closed-Circuit Television Systems as elements of Advanced Traffic Management Systems. This Policy provides principles which will be followed by the Department in the management of Traffic Management Systems.

III. Definitions.

A. "Closed-Circuit Television System ("CCTV system")" shall mean a video camera system and/or network used to collect, transmit and monitor data electronically via a data stream and project such data onto a video monitor, television screen or other monitoring equipment. The CCTV system is a closed circuit in that it has limited access and all elements are directly connected and controlled by authorized operators of the system. Directly connected in this context includes systems linked by microwave, infrared beams, electric wiring, etc.

B. "Advanced Traffic Management Systems ("ATM Systems")" shall mean technologies such as CCTV, traffic detectors and electronic message signs to collect information, manage traffic, quickly detect incidents, dispatch the proper response and provide motorists advanced notice of congestion, reducing the possibility of secondary accidents and allowing motorists to consider alternate routes, modes, or travel times.

C. "Transportation Management Center ("TMC")" shall mean the central station site for monitoring, analyzing and using the data collected by the Advanced Traffic Management System.

D. "Data" shall mean information collected by a CCTV system, including a live feed or any recording from such, from the Advanced Traffic Management System closed-circuit television system.

E. "Entity" shall mean a private corporation or other private organization, including media or other information service provider, which is duly authorized under an agreement with the Department consistent with this policy to receive Advanced Traffic Management System data.

F. "Incident" shall mean an activity that occurs on the road, roadway, right-of-way or in proximity to it, such as a vehicular accident, flat tire, fire, or similar situation that has or could have a roadway safety or congestion impact on travel conditions on such roadway.

G. "Personal Identifier Information" shall mean any data that
i. identifies an individual, drivers or passengers
ii. identifies license plate of vehicles
iii. identifies contents of the enclosed interior of passenger vehicles
iv. tracks the individual travel pattern of a specific vehicle

H. "Public Partner" shall mean any public agency, government, municipality, authority, accredited academic institution or coalition of such bodies that enters into an agreement with the Department for

Figure 27: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 2 of 11). (Source: New York State Department of Transportation)

the use of CCTV data consistent with the provisions set forth in this policy.

I. "Mine/Mining " shall mean any process wherein data containing personal identifier information is collected, manipulated, enlarged, enhanced, analyzed, and/or otherwise used.

IV. Principles.

The planning, design, deployment, operation and maintenance of all CCTV systems deployed by the Department, as elements of ATM System shall conform to the following principles:

A. Privacy.

The individual's right of personal privacy shall be respected and protected. The Department shall consider the protection of personal privacy in all aspects of system planning, design, deployment, operation, and maintenance and shall not collect or disseminate any personal identifier information, except as set forth herein. CCTV systems shall be used only as needed to perform necessary transportation planning, traffic management and traveler information functions as defined in this policy and shall not be used to monitor persons or private property, except as provided for in VI. A. 1 of this policy. In addition, CCTV systems shall not be used to monitor individuals or groups in a discriminatory manner contrary to applicable state law. The Department shall provide for a level of privacy consistent with reasonable expectations and the requirements of using CCTV systems for traffic management and traveler information purposes.

For purposes of this policy, the Department defines providing for a "reasonable expectation of privacy" as implementation of CCTV systems design and management and operational procedures, which do not include the collection of personal identifier information as defined in this policy, except as specifically provided for herein. This means that the Department shall take all reasonable efforts to ensure that CCTV systems shall not be used to collect personal identifier information consistent with this policy.

CCTV systems may collect this personal information, on an exception basis, only when such is needed to provide for the safety of the public and/or to perform necessary traffic planning and management functions such as zooming in on an incident to determine accident severity and appropriate emergency response, or where all personal information is subsequently removed from the data which is then used in an aggregated fashion, such as for the development of origin and destination data for transportation planning purposes.

B. Visibility.

ATM Systems shall be built in a manner visible to pedestrians, individuals and motorists. The public shall be made aware of projects to initially deploy or significantly expand CCTV systems on a facility, in

Figure 28: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 3 of 11). (Source: New York State Department of Transportation)

a corridor or throughout a region either through the requirements of the project design process, i.e. design report, public hearing, SEQRA process or through specific advisement via the local media and/or municipality, except where such advisement is not practical such as in the case of a temporary installation for purposes such as short term traffic management, construction or data collection, or where the installations are an element of routine-type maintenance activities. The Department shall disclose to the public information on these projects including location of cameras, the type of camera views that will be monitored, how information is collected, how the information shall be utilized and how such information shall be distributed. The Department shall provide timely public notice and consider public input in the planning and design of each of the systems in accordance with the State Environmental Quality Review Act ("SEQRA") process and this policy. If the installation of CCTV systems is such that the installation may result in a significant erosion of the public's reasonable expectation of privacy, as defined in this policy, on or in the vicinity of the highway, roadway and adjoining property, then such action shall be reviewed as an action having an effect on abutting properties or established human activities. Accordingly, the Department shall prepare an environmental assessment of such an action in accordance with 17 NYCRR section 15.6. Furthermore, the public shall be invited to observe the functioning of the CCTV systems from within the TMC, or other central gathering site for traffic information.

C. Security/Integrity.

Data security shall be designed into each CCTV system at the system architecture level. For the purpose of protecting personal identifier information, CCTV systems shall make use of hardware and software security technology, and audit procedures. ATM Systems shall use operational, technological and administrative safeguards to assure that access to personal identifier information is restricted to duly authorized individuals. Cameras shall be operated in a wide angle view that does not collect personal identifier information. When it is necessary to zoom a camera in a way that personal identifier information may be collected, dissemination of such data shall be discontinued until such time as the camera is returned to a view where personal identifier information is not being collected except as provided in VI. A. 2 and VI. A. 6 of this policy. Data shall be protected from improper alteration, manipulation or improper destruction. Security software and hardware will be consistent with the state of the art within the industry, as feasible for upholding the principles set forth in this policy.

The use of technology based privacy solutions is preferred, except where impracticable. The Department shall conduct a pilot project in Region 8 as set forth in the attached Addendum, in a timely manner, to examine and assess such technology-based solutions in an operating ATM system. The Department shall produce a pilot project evaluation report assessing the privacy solutions based on a number of factors including technological and operation considerations and cost. The Department shall conduct a study or studies assessing the feasibility of implementing the privacy solutions used in Region 8 in each of the other Department Regions. The study or studies shall include an analysis and recommendation for implementing such solutions in each of the Department Regions. Nothing shall restrict the Department from implementing such technology based solutions at an earlier date.

Figure 29: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 4 of 11). (Source: New York State Department of Transportation)

D. Extent/Use

CCTV systems shall be aimed and focused to collect only the minimum amount of information as necessary for transportation planning, traffic management and traveler information purposes. CCTV data shall only be used for the specific purposes set forth in this policy and with prior disclosure to the public. The Department may share CCTV views with other public partners to achieve common transportation objectives in improving transportation planning, traffic management and traveler information.

Data sharing in accordance with statewide regulations and this policy will be done to promote the performance of those functions, and only pursuant to written agreements that provide for the protection of personal privacy consistent with this policy. The agreements shall limit use of CCTV data to prescribed purposes, shall restrict the ability to record, retransmit, enhance or mine data from the CCTV systems and further preclude knowingly distributing any data that may contain personal identifier information. The Department shall discontinue the dissemination of data to any entity if the privacy protections set forth herein are not followed.

The Department may also distribute CCTV data directly to the public via the internet or other means for the purpose of providing traveler information. The Department shall take all reasonable efforts to ensure that any CCTV data disseminated in this manner shall not provide personal identifier information as previously defined in this policy. The sole purpose of providing such data shall be for the dissemination of traveler information to facilitate traffic management and the efficient balancing of transportation infrastructure demand and supply and all such uses and dissemination shall be consistent with statewide regulations, and this policy.

E. Access/Accountability/Retention.

Internal access to data shall be available only to authorized personnel. Authorization of access will be based on a work-related need and will include Department traffic operations personnel, agents of the Department involved in ATM system management, operations and maintenance, and duly authorized public partners. This will not preclude internal distribution to the general employee population within the Department of the same data as is available to the public for traveler information purposes via the internet, media or traveler information service providers. Visits by members of the general public to TMC shall be permitted.

Access to CCTV and ATM systems shall be controlled by pre-determined administrative and supervisory policies based on design and operational considerations and shall be tracked for adherence to procedures. Disciplinary procedures shall be established to address improper access, data manipulation, mining or data disclosure, as well as for assessment of procedural security. Procedures shall be developed to ensure appropriate training of personnel with access to CCTV systems and other

Figure 30: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 5 of 11). (Source: New York State Department of Transportation)

instrumentation with respect to the requirements of this policy.

Data shall not be recorded except in accordance with this policy.

In all cases, recording shall be done in accordance with this policy and shall be retained only for the minimum possible time frame after use of the archived data for its intended purpose, in accordance with the applicable Record Retention Authorization. Recorded data shall not include personal identifiers unless absolutely necessary to accomplish the intended purpose. Routine archiving of CCTV data shall not be part of the operational procedures and any recorded data shall be addressed in accordance with the Record Retention Authorization. Public access to any temporarily archived CCTV data shall be in accordance with applicable state law.

F. Commercial Use.

CCTV data may be shared with other entities for commercial use in order to provide for the widest distribution of the information to allow travelers to make informed travel decisions. For this purpose, the entity shall be regularly involved in the distribution of traveler information for commercial purposes and provides significant value to the Department in providing for widespread dissemination of traveler information to the public.

The Department shall take all reasonable efforts to ensure that any CCTV data as disseminated to these entities, shall not provide personal identifier information. The sole purpose of providing such data to these entities shall be for the dissemination of transportation information to facilitate traffic management and the efficient use of the transportation infrastructure and all such uses and dissemination shall be consistent with this policy. Dissemination of data shall only be done by written agreement containing privacy protection language consistent with this policy. The agreement shall limit the entities use of the CCTV data to prescribed purposes, shall prohibit their ability to enhance, mine, analyze and utilize personal identifier information from the data, shall restrict their ability to record, resell or retransmit the video and further preclude them from knowingly distributing any data that may contain personal identifier information as defined in this policy. Any agreements entered into by the Department with any other entity shall expressly provide that such agreement will be void if the entity fails to adhere to the privacy protections set forth in this policy. The Department shall discontinue the sharing of data if the privacy protection criteria are not adhered to.

G. Enforcement.

CCTV systems should be designed and used primarily for the traffic management and traveler information purpose for which they were installed and for which the public would reasonably expect. Enforcement agencies play an important public safety role in incident management activities. Accordingly, the Department partners and sometimes co-locates at TMCs with enforcement agencies to provide for the best incident management service to the public. As a result, enforcement agencies

Figure 31: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 6 of 11). (Source: New York State Department of Transportation)

may have access to CCTV data directly or remotely through TMCs for the purpose of coordinating incident management and incident-related public safety activities, and such is not provided for routine or regular monitoring for enforcement purposes. The ongoing sharing of data with enforcement agencies shall be documented by written agreement containing privacy protection language consistent with statewide regulations and this policy. Enforcement agencies shall be responsible for ensuring that any use of the CCTV systems is done in accordance with statutory authority, appropriate legal process, or emergency circumstances as defined by law.

V. Design and Operations Guidelines.

The following principles and guidelines shall apply to the Department's use of CCTV systems on its roadways:

A. TMC Policy Implementation.

1. Each region with an ATM system which includes CCTV systems shall designate a person responsible for the implementation and ongoing compliance with this policy including monitoring of local system design and operation to accommodate system and technology changes consistent with this Policy.

2. Such person shall be at least a grade level SG 24 and should be either the Regional Traffic Engineer, the Assistant Regional Traffic Engineer or the TMC manager.

3. Such person shall be responsible for monitoring research of the latest hardware and software technology for CCTV systems which are consistent with the design of the system, the policies set forth in this Policy, and shall implement into the local CCTV systems such feasible technologies necessary for upholding the principles set forth in this Policy.

B. Deployment of CCTV.

1. The public shall be made aware of projects to initially deploy or significantly expand CCTV systems at a facility, in a corridor or throughout a region in accordance with applicable requirements of this Policy.

C. Location of CCTV System Cameras.

1. Cameras shall be placed to provide the best available viewing of the roadway section, taking into account existing physical restrictions and topography.

2. Cameras should generally be installed in areas of traffic safety concerns and/or traffic congestion.

Figure 32: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 7 of 11).
(Source: New York State Department of Transportation)

3. CCTV systems should generally be installed in conjunction with other ATM system elements including variable message signs, highway advisory radio, traffic detectors, etc. to provide for transportation planning, traffic management and traveler information needs.

4. CCTV system cameras shall not be concealed and shall be installed at locations which provide an open view of the camera from the roadway, except as necessary and in response to accommodating public concern with roadside aesthetics.

VI. Operation of CCTV Systems.

A. CCTV Operations

1. No CCTV system shall monitor persons or private property, provided however, this provision shall not prohibit such monitoring on or adjacent to the roadway or right-of-way where it is not practical to avoid such monitoring during CCTV operation as provided in this policy, and this provision shall not prohibit such monitoring in the event of a public health danger or safety emergency, and this provision shall not prohibit the viewing of traffic-related conditions in plain view only as necessary for the Department to perform its traffic management activities as provided in this policy.

2. Personal identifier information data shall not be collected by the CCTV system, except that such data may be collected to provide for the safety of the public, respond to incidents, and the performance of necessary traffic and planning management functions.

3. CCTV systems shall operate in a wide-angle view mode which shall enable operators to view a large segment of the roadway without providing the ability to view any personal identifier information except as provided in Section IV. A. 2 or otherwise provided herein.

4. CCTV systems shall have physical and/or software controls which shall restrict the viewing area to the extent practical to that required for the intended traffic/incident management function.

5. CCTV systems shall only be used in a zoom mode where personal identifier information may be being collected on an exception basis, as defined in this policy. CCTV systems shall be returned to a view not containing personal identifiers when the need for such zooming has been met.

6. In the event of a public health danger or safety emergency, the Department may provide personal identifier information to such other public partner and/or entities as may be necessary to prevent, limit or mitigate such emergency.

Figure 33: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 8 of 11). (Source: New York State Department of Transportation)

B. Recording of CCTV System Video.

1. Except as provided for in this policy, CCTV data shall not be recorded and all data disseminated from CCTV systems shall be transferred in a real time or limited time delay data feed. In all cases, recording shall only be done in a manner that protects the privacy of the public in accordance with this policy.

2 CCTV data shall only be recorded in response to a specific need where a review of the data would contribute to improving safety and/or future traffic operations procedures or system planning and performance including:
i. review of a traffic operations or safety problem;
ii. provision of a training review for future operator training;
iii. research activities that will improve future technology or operations;
iv. post-incident review of a particularly complex incident and emergency response for the purposes of improving operational procedures and response;
v. demonstrating or testing equipment or system functions; or
vi. collection of data for transportation planning management purposes where personal identifier information is subsequently removed from the data.

3. If a recording is made, it shall be retained in a specifically designated and secure location with access restricted by supervisory level personnel.

4. CCTV system data which have been recorded shall be retained only for the minimum possible time after use of the archived data for its intended purpose in accordance with the applicable Department Records Retention Authorization.

C. Training and Accountability.

1. All operators shall be trained and certified in the proper operation of the CCTV systems according to the policy and principles set forth in this policy. Such certification shall be required before operators are allowed to operate CCTV systems. Operator training shall be maintained as an evolving, continuous process.

2. Each TMC shall have a written procedures manual for operation of CCTV systems. This manual shall include the principles and policy set forth in this policy, and may either be a part of an overall TMC Operations Manual or a specific CCTV system Operations Manual.

3. All TMC personnel authorized to operate the CCTV system shall be provided with a copy of the operations manual, and verify in writing that they have received it , reviewed it and agree to follow the procedures in the manual.

Figure 34: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 9 of 11).
(Source: New York State Department of Transportation)

4. Disciplinary criteria shall be established for personnel who knowingly violate the established CCTV system operations procedures and principles or policy set forth in this policy, regardless of the agency or entity by whom they are employed. Department personnel shall be disciplined in accordance with appropriate personnel procedures. Any contracts with firms involving the operation of CCTV for the Department shall include appropriate language requiring conformance with this policy and identifying an acceptable disciplinary procedure. The disciplinary procedures shall be a part of the TMC or CCTV system operations manual.

VII. Agreements

The Department shall not provide CCTV data containing personal identifier information to any public partner except for the purposes set forth in VI. A. 2 and VI. A. 6 of this policy, or to a private entity except for the purposes as set forth in VI. A. 6 of this policy at any time, provided, however that the Department may provide such data, consistent with this policy, to consultants retained by the Department in the performance of Department functions. The sole purpose of providing such data shall be for the dissemination of transportation information to facilitate traffic management and the efficient use of the transportation infrastructure and all such uses and dissemination shall be consistent with this policy.

A. No data shall be shared or otherwise disseminated except in accordance with this policy.

B. Any agreement entered into by the Department with any public partner or entity, except as otherwise provided in this policy, shall provide that there shall be no dissemination of data containing personal identifier information to any third party without written agreement containing privacy protection language consistent with this policy. Such agreement shall limit the use of the CCTV data to prescribed purposes consistent with this policy, and shall prohibit the mining of such data.

C. Any agreements entered into by the Department with any public partner or entity shall expressly provide that the party to such agreement shall no longer receive data if the entity fails to adhere to the privacy protections set forth in this policy.

D. The Department may terminate any agreement or execution of such agreement that does not conform with the provisions of this regulation.

E. Agreements entered into under this policy shall provide the Department with complete authority and retain control over the CCTV systems data that is provided to other public partners, entities and the public, including when it shall be made available. Such agreements shall provide that when CCTV systems collect personal identifier information, data feed to any entity shall be discontinued until such time as the CCTV systems is returned to a mode where personal

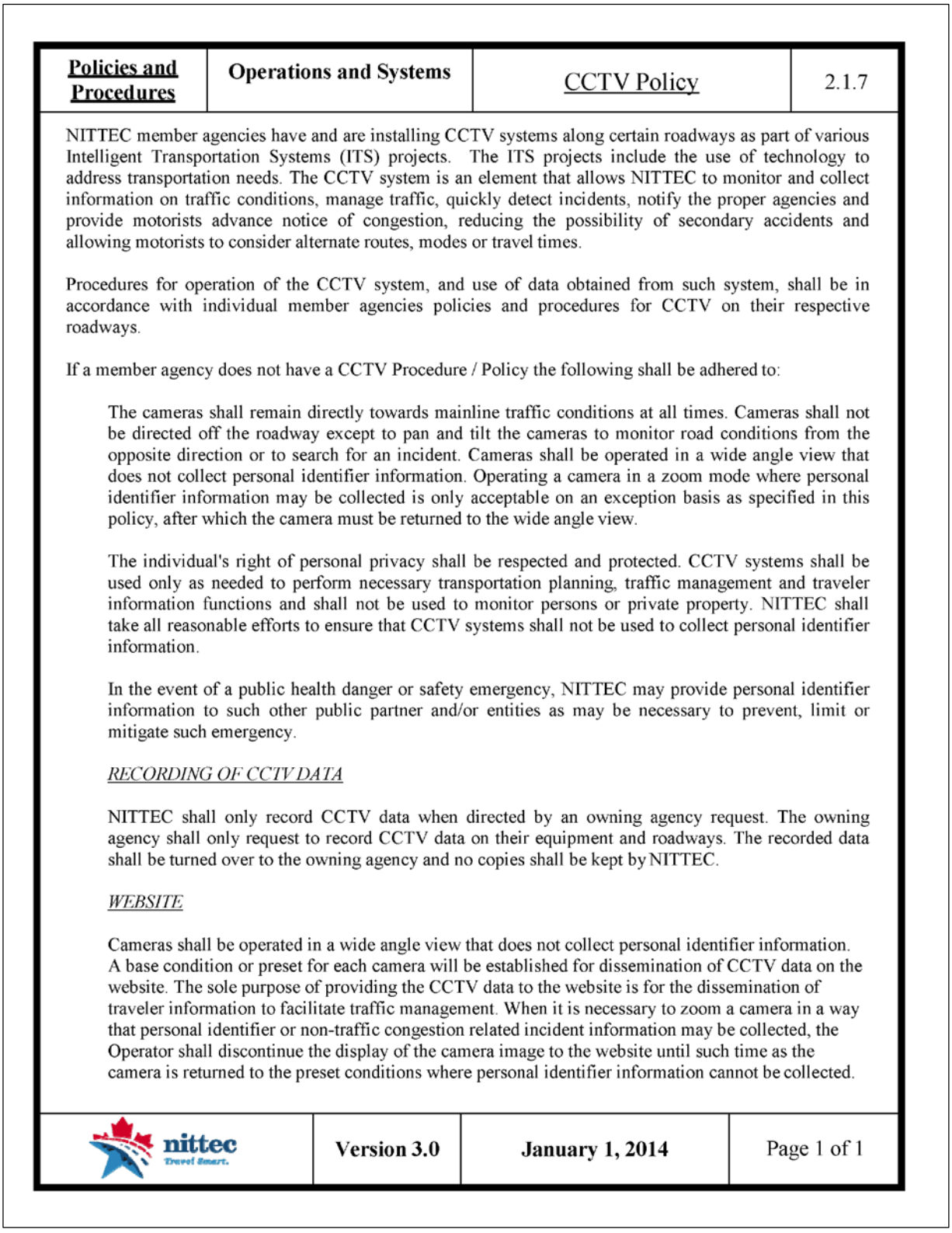
Figure 35: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 10 of 11). (Source: New York State Department of Transportation)

identifier information is not being collected except as provided in VI. A. 2 and VI. A. 6 of this policy.

F. Agreements entered into under this policy shall provide that entities receiving data shall not have the right to re-transmit, enhance for personal identification, mine or otherwise modify data containing personal identifier information.

G. All agreements between public partners or entities and third parties for receipt of CCTV data shall be consistent with the privacy restrictions and policies of this policy.

Figure 36: Sample scan. Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems (page 11 of 11).
(Source: New York State Department of Transportation)



Policies and Procedures	**Operations and Systems**	CCTV Policy	2.1.7

NITTEC member agencies have and are installing CCTV systems along certain roadways as part of various Intelligent Transportation Systems (ITS) projects. The ITS projects include the use of technology to address transportation needs. The CCTV system is an element that allows NITTEC to monitor and collect information on traffic conditions, manage traffic, quickly detect incidents, notify the proper agencies and provide motorists advance notice of congestion, reducing the possibility of secondary accidents and allowing motorists to consider alternate routes, modes or travel times.

Procedures for operation of the CCTV system, and use of data obtained from such system, shall be in accordance with individual member agencies policies and procedures for CCTV on their respective roadways.

If a member agency does not have a CCTV Procedure / Policy the following shall be adhered to:

The cameras shall remain directly towards mainline traffic conditions at all times. Cameras shall not be directed off the roadway except to pan and tilt the cameras to monitor road conditions from the opposite direction or to search for an incident. Cameras shall be operated in a wide angle view that does not collect personal identifier information. Operating a camera in a zoom mode where personal identifier information may be collected is only acceptable on an exception basis as specified in this policy, after which the camera must be returned to the wide angle view.

The individual's right of personal privacy shall be respected and protected. CCTV systems shall be used only as needed to perform necessary transportation planning, traffic management and traveler information functions and shall not be used to monitor persons or private property. NITTEC shall take all reasonable efforts to ensure that CCTV systems shall not be used to collect personal identifier information.

In the event of a public health danger or safety emergency, NITTEC may provide personal identifier information to such other public partner and/or entities as may be necessary to prevent, limit or mitigate such emergency.

RECORDING OF CCTV DATA

NITTEC shall only record CCTV data when directed by an owning agency request. The owning agency shall only request to record CCTV data on their equipment and roadways. The recorded data shall be turned over to the owning agency and no copies shall be kept by NITTEC.

WEBSITE

Cameras shall be operated in a wide angle view that does not collect personal identifier information. A base condition or preset for each camera will be established for dissemination of CCTV data on the website. The sole purpose of providing the CCTV data to the website is for the dissemination of traveler information to facilitate traffic management. When it is necessary to zoom a camera in a way that personal identifier or non-traffic congestion related incident information may be collected, the Operator shall discontinue the display of the camera image to the website until such time as the camera is returned to the preset conditions where personal identifier information cannot be collected.

nittec Travel Smart.	**Version 3.0**	**January 1, 2014**	Page 1 of 1

Figure 37: Sample scan. Niagara International Transportation Technology Coalition (NITTEC) Closed-Circuit Television (CCTV) Policy (page 1 of 1).
(Source: NITTEC)

Oregon Department of Transportation ***Transportation Operations Center Standard Operating Guideline***	NUMBER: **50.3.1**	SUPERSEDES: **November 1, 2003**
	EFFECTIVE DATE: **April 16th, 2014**	PAGE: **1**
	REVIEW AND VALIDATION DATE: **April 16th, 2014**	
SUBJECT: **Use of CCTV Highway Cameras**	REFERENCES: **See Below**	

PURPOSE: **Establish standard operating guidelines for the use of closed circuit TV cameras (CCTV).**

GUIDELINE:

1. The number of CCTV cameras on Oregon highways is increasing annually. These cameras assist ODOT Transportation Operations Centers (TOCs) in monitoring traffic and incidents on Oregon highways. The majority of the cameras belong to ODOT. There are a few joint use agreements allowing multiple agencies to control a single camera. Captured images can be viewed by the general public via the ODOT internet web page and TripCheck. In respect for the privacy concerns of the public, these CCTV camera operating guidelines should be followed:

    a. CCTV cameras will be set to view public right-of-way and zoomed out to view a sizable portion of the highway when not in use.

    b. CCTV cameras will only be used to zoom in close enough to gather necessary information. Cameras will not be used to zoom in on individuals, especially where injuries are involved.

    c. CCTV cameras will not be used to view the general public when not associated with an ODOT or law enforcement operation.

    d. CCTV cameras will not be used to view any part of privately owned property; homes, businesses and etc.

    e. CCTV cameras will not be used to zoom in on police activities occurring on or off the highways. Cameras may be used to aid law enforcement or provide additional eyes for safety. Cameras must be zoomed out or away immediately once requested assistance is rendered or sufficient officers to control the situation are on scene.

    f. CCTV data will generally not be recorded or archived. Exceptions include cameras installed specifically for security and occasional recording for research or traffic analysis needs. Recorded images are considered public information and can be used as evidence.

UPDATES AND CHANGES

Contact the ITS Operations Coordinator 503-986-6568 with recommended updates and changes.

1

Figure 38: Sample scan. Use of Closed-Circuit Television Highway Cameras Guidelines at the Oregon Department of Transportation (page 1 of 1).
(Source: Oregon Department of Transportation)

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 real-time traffic condition information, TDOT has constructed and operates four Regional Traffic 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.

Figure 39: Sample scan. Access to Tennessee Department of Transportation's Live Video Feeds and Information Sharing Policies (page 1 of 1).
(Source: Tennessee Department of Transportation)

Tennessee Department of Transportation
And
Responder 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 real-time 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 pursuant to section 2.I.

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.

Page 1 of 6

Figure 40: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 1 of 6).
(Source: Tennessee Department of Transportation)

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 image 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 files 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:**

   A. 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

Page 2 of 6

Figure 41: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 2 of 6).
(Source: Tennessee Department of Transportation)

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.

B. USER shall maintain the security and integrity of the CCTV system by limiting use of the system to trained and authorized individuals within their agency, 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.

C. USER accepts all risks inherent with the live video feeds, including, but not limited to, interruptions in the video feeds, 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. To the extent permitted by applicable law, 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.

D. 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.

E. USER agrees to acknowledge that the video feeds are provided by the Tennessee Department of Transportation.

F. USER agrees to display the SMARTWAY logo in the upper right hand corner of any view provided outside of the agency.

G. USER agrees to actively participate in the National Traffic Incident Management Responder Training Program. USER agrees that any employee of the agency reporting to the scene of an incident shall attend one 4-hour, in-person, National Traffic Incident Responder Training Program session within one year of the signing of this document. Training sessions will be provided for free and coordinated between the USER and TDOT.

H. USER agrees to support and abide by the concept of a safe and quick clearance approach to traffic incidents and events, as defined by the National Traffic Incident Responder Training Program.

Page 3 of 6

Figure 42: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 3 of 6).
(Source: Tennessee Department of Transportation)

I. 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 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.

J. USER agrees to actively participate in quarterly Regional Traffic Incident Management meetings. USER agrees to provide the names of a primary and alternate individual with the authority to speak on behalf of the USER at these quarterly meetings.

3. **LIABILITY AND INDEMNITY PROVISIONS:**

A. To the extent permitted by applicable law, 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.

B. 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

Figure 43: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 4 of 6).
(Source: Tennessee Department of Transportation)

privacy occurring as a proximate result of information made available from the CCTV system.

4. **TERMINATION:**

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

Figure 44: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 5 of 6).
(Source: Tennessee Department of Transportation)

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:_____

Page 6 of 6

Figure 45: Sample scan. Responder Entity Users Access Agreement for Live Video and Information Sharing (page 6 of 6).
(Source: Tennessee Department of Transportation)

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 real-time 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.

Page 1 of 5

Figure 46: Sample scan. Private Entity Users Access Agreement for Live Video and Information Sharing (page 1 of 5).
(Source: Tennessee Department of Transportation)

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:**

   A. 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

Figure 47: Sample scan. Private Entity Users Access Agreement for Live Video and Information Sharing (page 2 of 5).
(Source: Tennessee Department of Transportation)

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.

B. 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.

C. 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.

D. 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.

E. USER agrees to acknowledge that the video feeds are provided by the Tennessee Department of Transportation.

F. USER agrees to display the SMARTWAY logo in the upper left hand corner of any view provided outside of the agency.

G. 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

Figure 48: Sample scan. Private Entity Users Access Agreement for Live Video and Information Sharing (page 3 of 5).
(Source: Tennessee Department of Transportation)

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.

H. 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:**

A. 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.

B. 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:**

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

Figure 49: Sample scan. Private Entity Users Access Agreement for Live Video and Information Sharing (page 4 of 5).
(Source: Tennessee Department of Transportation)

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_____

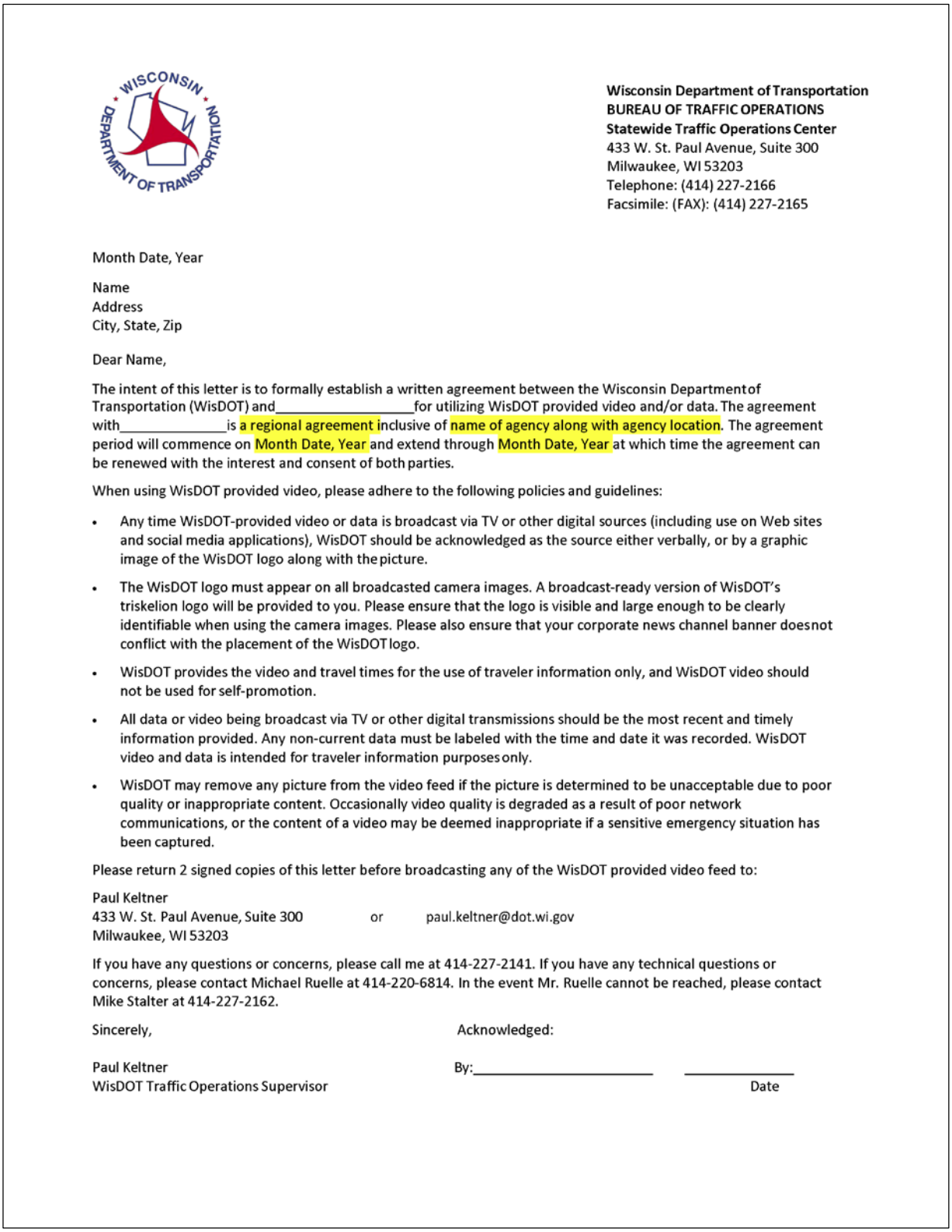
(Print Name)_____

(Title)_____

Date:_____

Page 5 of 5

Figure 50: Sample scan. Private Entity Users Access Agreement for Live Video and Information Sharing (page 5 of 5).
(Source: Tennessee Department of Transportation)



Wisconsin Department of Transportation
BUREAU OF TRAFFIC OPERATIONS
Statewide Traffic Operations Center
433 W. St. Paul Avenue, Suite 300
Milwaukee, WI 53203
Telephone: (414) 227-2166
Facsimile: (FAX): (414) 227-2165

Month Date, Year

Name
Address
City, State, Zip

Dear Name,

The intent of this letter is to formally establish a written agreement between the Wisconsin Department of Transportation (WisDOT) and_____for utilizing WisDOT provided video and/or data. The agreement with_____is a regional agreement inclusive of name of agency along with agency location. The agreement period will commence on Month Date, Year and extend through Month Date, Year at which time the agreement can be renewed with the interest and consent of both parties.

When using WisDOT provided video, please adhere to the following policies and guidelines:

- Any time WisDOT-provided video or data is broadcast via TV or other digital sources (including use on Web sites and social media applications), WisDOT should be acknowledged as the source either verbally, or by a graphic image of the WisDOT logo along with the picture.
- The WisDOT logo must appear on all broadcasted camera images. A broadcast-ready version of WisDOT's triskelion logo will be provided to you. Please ensure that the logo is visible and large enough to be clearly identifiable when using the camera images. Please also ensure that your corporate news channel banner does not conflict with the placement of the WisDOT logo.
- WisDOT provides the video and travel times for the use of traveler information only, and WisDOT video should not be used for self-promotion.
- All data or video being broadcast via TV or other digital transmissions should be the most recent and timely information provided. Any non-current data must be labeled with the time and date it was recorded. WisDOT video and data is intended for traveler information purposes only.
- WisDOT may remove any picture from the video feed if the picture is determined to be unacceptable due to poor quality or inappropriate content. Occasionally video quality is degraded as a result of poor network communications, or the content of a video may be deemed inappropriate if a sensitive emergency situation has been captured.

Please return 2 signed copies of this letter before broadcasting any of the WisDOT provided video feed to:

Paul Keltner
433 W. St. Paul Avenue, Suite 300 or paul.keltner@dot.wi.gov
Milwaukee, WI 53203

If you have any questions or concerns, please call me at 414-227-2141. If you have any technical questions or concerns, please contact Michael Ruelle at 414-220-6814. In the event Mr. Ruelle cannot be reached, please contact Mike Stalter at 414-227-2162.

Sincerely,

Paul Keltner
WisDOT Traffic Operations Supervisor

Acknowledged:

By:_____ _____
Date

Figure 51: Sample scan. Video Utilization Agreement (page 1 of 1).
(Source: Wisconsin Department of Transportation)

ACKNOWLEDGMENTS

We would like to acknowledge the following Transportation Management Center (TMC) Pooled Fund Study (PFS) members for their contribution, support, and technical guidance during this project:

- Donald Gedge—Tennessee Department of Transportation.
- Jeff Galas—Illinois Department of Transportation.
- Jeremy Iwen—Wisconsin Department of Transportation.
- John Bassett—New York State Department of Transportation.
- John McClellan—Minnesota Department of Transportation.
- Luke Biernbaum—Michigan Department of Transportation.
- Ming Shuin Lee—AECOM.
- Paul Keltner—Wisconsin Department of Transportation.
- Vinh Dang—Washington State Department of Transportation.

We would also like to thank additional participants for their Case Study input:

- Sinclair Stolle—Iowa Department of Transportation.
- Michael Juliano—New Jersey Department of Transportation.
- Brian Hoeft—Regional Transportation Commission of Southern Nevada.
- Scott Kozlick—Wisconsin Department of Transportation.

U.S. Department of Transportation
Federal Highway Administration
Office of Operations
1200 New Jersey Avenue, SE
Washington, DC 20590

www.ops.fhwa.dot.gov

March 2016

FHWA-HOP-16-033