Video Quality in Public Safety (VQiPS):

Policy Considerations for the Use of Video in Public Safety

First Responders Group

June 2016

Homeland Security

Science and Technology

Intentionally Blank

VQiPS Report

Policy Considerations for the Use of Video in Public Safety

HSHQPM-15-X-00122
June 2016

Prepared for:	**The First Responders Group Office for Interoperability and Compatibility**
Prepared by:	**Johns Hopkins University Applied Physics Lab with support from VQiPS Working Group's Policy Subcommittee**

Intentionally Blank

Prepared for:

Department of Homeland Security Science and Technology Directorate
Washington, DC

This document was prepared under funding provided by the U.S. Department of Homeland Security Science and Technology Directorate (Resilient Systems for Public Safety Communication). Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) assumes no liability for this document's content or use thereof. This document does not constitute a standard, specification or regulation. Additionally, JHU/APL does not endorse particular products or manufacturers. Trade and manufacturer's names may appear in this report only because they are considered essential to the object of this document.

Principal Author: Don Zoufal (VQiPS, SDI Solutions)
Contributing Authors: Julie Stroup (VQiPS, City of Houston Texas), Mark Ryckman (VQiPS, City of Corning New York), John Garofolo (VQiPS, NIST), Hinrich Schmidt (VQiPS, Motorola Solutions), Tom Hengeveld (VQiPS, Harris), Mike Fergus (VQiPS, IACP), Andrew Hartigan (CSRA/DHS), John Contestabile (JHU/APL), Steven Babin (JHU/APL), and other members of the Video Quality in Public Safety (VQiPS) Policy Subcommittee.

Publication Notice

Disclaimer

The views and opinions of authors expressed herein do not necessarily reflect those of the U.S. government.

Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. government.

With respect to documentation contained herein, neither the U.S. government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed; nor do they represent that its use would not infringe privately owned rights.

Contact Information

Please send comments or questions to: SandTFRG@HQ.DHS.GOV

Intentionally Blank

TABLE OF CONTENTS

Contents

Disclaimer 6

Contact Information 6

TABLE OF CONTENTS 8

EXECUTIVE SUMMARY 10

INTRODUCTION & BACKGROUND 11

POLICY FRAMEWORK 12

OVERARCHING SUBSTANTIVE ISSUES 13

Public Safety Goals 13

Privacy Issues 16

Security Issues 18

Transparency Issues 19

Common Technical Issues in Operations of Public Video systems 21

Technology Considerations for Video Data 21

Interoperability for Video Data Sharing 26

Continuity of Operation (COOP) 27

ISSUE ANALYSIS 28

Issue Analysis Format 28

Issue Discussions 29

1. Sighting and Location Considerations 29
2. Access and Use (Real-Time and Forensic) of Video Systems and Data 38
3. Sources Considerations 47
4. Notice Considerations 53
5. Monitoring, Analysis and Analytic Applications 57
6. Retention of Video Data (Imagery and Metadata) 61
7. Dissemination of Video Data (Imagery and Metadata) 66
8. A Well Defined Governance Structure is Important for Video Program Success 72

CONCLUSIONS 76

REFERENCES 78

APPENDIX 81

Intentionally Blank

EXECUTIVE SUMMARY

This document represents the efforts of the Video Quality in Public Safety (VQiPS) Working Group's Policy Subcommittee to provide guidance for government agencies crafting written policies and procedures for the use of closed circuit television (CCTV) video data and metadata in a variety of public safety applications. This Subcommittee, consisting of experts in many areas of public safety, held meetings in person and via teleconference over several months in 2015 and 2016 to discuss important policy issues related to CCTV use. The purpose was not to provide a template or best practices document, but instead to highlight policy considerations for agencies in the process of establishing or implementing recently established video systems. These considerations might also be useful for agencies that have older video systems, but want to examine whether their established policies reflect the current social and legal environment.

This document is organized into five sections. The first section provides background information on the VQiPS Working Group's involvement in the public safety uses of CCTV video. The second section introduces the Policy Framework. The Policy Subcommittee made a specific choice to focus this framework on the use of video by governmental entities in public spaces because of the inherent policy challenges. They decided not to focus on the use of any particular camera or system (i.e., permanent or temporary, fixed or mobile), but instead to capture issues that must be addressed in the implementation of a CCTV video program for public safety applications. The third section covers overarching substantive issues. These are issues the Subcommittee decided require consideration across virtually all aspects of a video program: clearly articulated public safety goals; understanding and accommodation of privacy concerns; attention to the security of video networks and data; transparency in the conduct of image collection and data storage and use; and common issues in the operation of public video programs, including technology considerations, interoperability and continuity of operation. The Issue Analysis section provides a detailed discussion of eight additional issues that the Policy Subcommittee determined require careful consideration by policy makers as they develop their video programs. Those issue areas are: 1) sighting and location; 2) access and use, including search; 3) source considerations; 4) notice considerations; 5) monitoring, analysis and analytic applications; 6) retention of data; 7) dissemination of data; and 8) governance issues. These issues are analyzed according to their underlying assumptions, strategic objectives, operational measures, technical measures, stakeholders, impacts and any other special considerations. Finally, the Conclusions section summarizes some important general points about developing CCTV video policies for government use. It should be emphasized that these policies need to be aligned with a clearly defined governmental purpose for the video system, as well as consistent with legal requirements and privacy concerns and protections.

Determining the government purpose(s) for a CCTV video system is essential. A written policy statement outlining public safety purposes and goals is an important step in demonstrating the public safety purpose(s) that the government seeks to accomplish. This document should serve

as a resource for issues to consider when formulating or updating government policies and procedures for the deployment, use, sharing and maintenance of CCTV video information and systems.

INTRODUCTION & BACKGROUND

First responders have come to rely on video technology to increase their situational awareness while onsite at an incident, remotely monitoring an incident or conducting day-to-day responses. As video technology has evolved, equipment options have become increasingly complex. Many first responder agencies lack the tools and subject matter expertise needed to make informed video system purchasing decisions, so they often turn to manufacturers to obtain information for their purchasing decisions. The Video Quality in Public Safety (VQiPS) Initiative provides useful information and support to the public safety and allied communities so they can articulate their own video quality needs, and ultimately buy the commercial products that best fit their unique requirements.

The VQiPS Initiative began in 2008 as a partnership between the U.S. Department of Homeland Security (DHS) Science and Technology Directorate and the U.S. Department of Commerce Public Safety Communications Research (PSCR) program. Through the creation of unbiased guidance and educational resources, VQiPS assists the public safety community in clearly defining and communicating their video quality needs. VQiPS empowers practitioners with the tools and information needed to purchase and deploy the appropriate video technology solutions to support their mission.

VQiPS is driven by a multi-faceted group of stakeholders composed of local, state and federal first responders from across various disciplines, federal partners, representatives from academia and standards-making bodies, and industry. Among its most noteworthy knowledge products, the VQiPS Working Group developed a User Guide web tool that assists practitioners in determining video options based on specific video scenes they will be targeting and the resulting tasks that need to be accomplished based on viewing that scene [1,2]. VQiPS also developed a glossary of video system terminology, a video library and the Digital Video Quality Standards Handbook [3]. Further guidance has been issued through numerous technical reports on topics such as *Optimizing Network Resources for Transmitting Video on Public Safety LTE* Networks [4].

As video becomes more universally used in the public safety community, it has also become increasingly apparent that there are factors beyond the technology itself that need to be considered. At the 2014 annual VQiPS Workshop, one of the issues that rose to the top of several discussions was the importance of video policy. Several of the case study panelists highlighted how their individual agency struggled with issues such as video retention, privacy

and chain of custody. This became the incentive for the establishment of a Policy Subcommittee within the VQiPS Working Group. What follows is the first deliverable from this group, which highlights policy considerations for agencies who may be in the process of establishing or deploying recently established video systems. These considerations might also be useful for agencies that have older video systems, but want to examine whether their established policies reflect the current social and legal environment.

POLICY FRAMEWORK

Consistent with its mission and vision statements (Figure 1), the VQiPS Policy Subcommittee has worked to create a policy *framework* for consideration by entities looking to collect and utilize closed circuit television (CCTV) video. It is not focused on the use of any particular camera or system (permanent or temporary, fixed or mobile), but is designed to generally capture issues that must be addressed in the implementation of a CCTV video program for public safety applications. It is also important to note that the Policy Subcommittee made a specific choice to focus this framework discussion on the *use of video by governmental entities in public space* because of the policy challenges of these users and their video uses. Many of the issues identified in this work have implications for the growing field of wearable cameras, but those uses raise additional concerns that are not addressed here. Similarly, private sector video users may benefit from examination of issues in this work, but it is not specifically targeted for video programs of those users.

VQiPS Vision:

The VQiPS Working Group will create a collaborative environment that accelerates the ability of users to specify and deploy video technology solutions that meet user requirements and improve public safety and homeland security enterprise operations.

VQiPS Mission:

The VQiPS Working Group creates knowledge products, fosters a knowledge-sharing environment, and supports research, development, testing and evaluation for enhanced video quality through measurable, objective and standards-based solutions across the full spectrum of video-use cases for the public safety community.

Figure 1. VQiPS Vision and Mission Statements.

The goal of the policy framework is not to provide a specific policy or process solution. User needs and the ways in which video can be utilized vary significantly between different users and

the way they use video. Policies should be flexible in order to address the needs of these differing users with differing uses of video. Nevertheless, every use of CCTV video has certain common issues and challenges.

This framework approach is an attempt to highlight areas of concern and accepted approaches for meeting those challenges. It is not a discussion of "best practices." It does not prescribe a model policy nor offer a universal template. Instead, it presents users with a set of considerations for the preparation of written policies and offers some approaches to meeting those challenges that other jurisdictions have used.

The VQiPS Policy Subcommittee believes that there is no "one policy" for addressing video use, but the development of a written policy is an *essential part* of a successful CCTV video program. Users must make policy decisions based on a complex matrix of use requirements, resource availability, and the constraints of local laws and regulations. However, while the resulting policy may vary from jurisdiction to jurisdiction, the process of developing an effective policy should address certain overarching issues.

OVERARCHING SUBSTANTIVE ISSUES

The Policy Subcommittee identified five overarching substantive issues that require consideration across virtually all aspects of a video program: clearly articulated public safety goals; understanding and accommodation of privacy concerns; attention to the security of video networks and data; transparency in the conduct of image collection and data storage and use; and common issues in the operation of public video programs, including technology considerations, interoperability and continuity of operation. Each issue is examined in detail below.

Public Safety Goals

As is true of all government programs, a central concern in the operation of a CCTV video system is ensuring that it is *aligned with a legitimate governmental purpose*. With respect to video programs, that governmental purpose generally falls within the purview of public safety. However, there are multiple aspects of governmental public safety operations that can benefit from information provided by video programs.

Traditional Video Usage Pre-9/11

Use of video monitoring is not a completely recent development. Government entities (as well as the private sector) have been using video in conjunction with governmental programs for many years. Traditional uses have included traffic control and management, physical security and use in high crime areas. Jurisdictions use video to monitor traffic operations in many large cities because such resources can help transportation professionals determine how to better

move traffic through roadway networks by providing traffic management personnel with better situational awareness or by adjusting signals and timing.

Another traditional governmental use of cameras is to assist in safeguarding the physical security of critical infrastructure and resources owned or operated by government entities. Common among these are government office buildings, courts and government-held utility facilities (water/wastewater and power). Use of video at these types of facilities has long been accepted as an integral part of a comprehensive physical security program.

CCTV video cameras have been used in high crime areas to deter crime and enhance public confidence in their safety. Under this premise, video cameras were placed in areas like public parking garages or commercial shopping areas. Municipal jurisdictions nationally and internationally experimented with using cameras to monitor public areas to promote the safety of activities like shopping and other commerce. Although some recent academic studies of these video programs show mixed success in preventing serious crime (e.g., [5]), the ability to view video of incidents after they occur has proven very beneficial in criminal investigations.

Video Usage Post-9/11

Post 9/11, there was a marked change in the public use of CCTV video. Three factors significantly influenced this changed usage: evolving technology; resource availability; and increased operational understanding of the value of improving situational awareness. As a result, government use of video has significantly expanded.

The revolution in video technology since 9/11 has allowed for more widespread use. Advances in camera technology, network technology, computing and a number of other related fields has allowed for the development and deployment of increasingly complex camera networks at increasingly lower price points. At the same time, the post 9/11 availability of funding for video programs was increased, particularly through federal government grant programs. Finally, the first responder community became more aware of the value of video technology as a tool to enhance situational awareness. The promise of an enhanced operating picture led to increased demand by the first responder community for more video.

Ordinary crime control has been an area of increasing expansion of video use. Within the purview of ordinary crime control, video systems can contribute valuable information to first responders. Visual imagery can provide first responders, dispatchers and supervisory personnel with important information on the nature of any incident, whether an emergency or a routine public safety response. That information can help to make the response more effective and efficient, and improve management of limited resources. Some cities are now looking to

interface public and private CCTV camera programs with their 9-1-1-dispatch operation, and even automate their interface with computer aided dispatch programs.

Video use for large-scale incident and event management and emergency management protocols has also expanded. Video images provide situational awareness that facilitates large crowd management. Video deployments can also contribute to a better understanding of incidents or events that may encompass a wide geographic area. This can be particularly useful for emergency management operations in furnishing information to incident command personnel regarding resource deployment and in supporting personnel as they attempt to anticipate operational requirements.

With respect to anti-terrorism efforts, video is seen as a tool to enhance physical security efforts and to harden potential targets. In the years since the events of 9/11, millions of dollars have been spent by federal, state, local, and tribal governments on deployments of CCTV video systems to help protect potential terrorist targets. Those systems have been deployed in a variety of ways across different types of facilities. They have ranged from extensive citywide networks in places like Chicago, New York and Baltimore, to smaller deployments more targeted at specific critical infrastructure and key resources (CIKR) facilities. Like some of the deployments meant to address ordinary crime control issues, these deployments have engendered debate over efficacy.

Finally, the value of recorded video after an incident must be considered. Review and analysis of video evidence was a critical component of the 2013 Boston Marathon bombing investigation [6]. More than 5,000 hours of video evidence capturing over 10,000 individual criminal acts were recovered following the Stanley Cup riot in Vancouver, Canada, in June 2011 [7]. Whether investigating a terror incident or a simple robbery, the quality of the recorded digital media evidence (DME) must be carefully considered to provide the level of detail necessary for probative value for investigators.

Public/Private Collaboration

Another phenomenon of camera use post 9/11 has been the development of collaborative public/private camera usage. The sharing of these images from public facing camera deployments on private property has been made possible by developments in both computing and camera technology. Those sharing arrangements may be through fixed networks like those found in the Lower Manhattan Security Initiative [8], or through ad hoc image sharing like those that occurred in the advent of the 2013 Boston Marathon Bombing incident [6]. Camera mapping and registration programs have started in a number of large and small jurisdictions allowing public safety personnel to leverage public facing cameras operated by private entities

and individuals. Governments, both large and small, have come to understand the efficiency of leveraging such public-facing private camera networks to augment their public safety efforts.

Critical to this growing and important information sharing initiative is the understanding that such sharing projects are for the advancement of security for public areas. That is, this sharing cannot be viewed as a program to provide enhanced security for private persons or entities. Therefore, the expectations of participating private sector entities need to be managed. Clear lines need to be drawn with respect to government use of private camera images. The images utilized should be of those cameras that cover public areas.

Measures to Ensure Pursuit of Public Safety Goals

Irrespective of the range of public safety purposes for which cameras are deployed, one thing seems clear. Communities expect that the cameras should only be used for certain approved government purposes. Therefore, government entities planning to deploy cameras or gather images from private cameras need to ensure that such activities align with an articulated legitimate government purpose.

A written policy statement outlining public safety purposes and goals is an important step in demonstrating the public safety purpose or purposes that government seeks to accomplish. However, such policy statements are only the beginning of the process to assure the public of the government's acceptable use of this information. Written policies need to be developed to ensure the integrity of the systems and that their use is only for a legitimate government purpose. Audit programs must be developed and implemented to ensure appropriate use in practice. Where misuse is identified, it must be met with properly documented corrective action, including the discipline of individuals involved in misuse. Like any other public safety tool, camera programs require strict compliance with written policy to ensure use is consistent with legitimate governmental interests.

Privacy Issues

The issue of privacy is one that pervades government use of video and video data from public space. As a general rule, under both federal and state law, there is no cognizable protection against observing and recording conduct occurring in a public space [9]. However, protection of privacy in public has been afforded in some circumstances, such as conversations in public places, where the individual can demonstrate a reasonable expectation of privacy in the conduct [10]. Additionally, there are clear concerns where enhanced technology is used in public space to observe private property [11]. Thus, where a video system is developed to observe public conduct, it needs to be limited in scope to public areas and cover only visual imagery and not audio voice recordings.

In addition to questions of what kinds of activity and conduct can be observed or recorded on video systems, the development of complex computer systems that can interrelate large amounts of public surveillance data poses additional potential issues. While the U.S. Supreme Court has not extended Constitutional protections of public data, review of some of those decisions demonstrate concern over potential privacy impacts of publicly collected data. Protection of publicly collected CCTV images is already the subject of regulation in the European Union under the auspices of the Data Protection Directive [12]. Privacy Acts that specifically mention CCTV video data have been passed in the United Kingdom [13] and New Zealand [14]. Statutory and regulatory schemes to protect that data in the U.S. are also being advocated (e.g., see [15], [16]). Accordingly, careful consideration needs to be given to management of the data collected.

Privacy concerns are present in the entire video lifecycle. Organizations deploying video surveillance systems should first develop policies that clearly indicate how video will be captured, analyzed, retained and disclosed, as each of these activities can have a significant privacy impact. Some organizations may be required to draft and publish formal privacy impact statements prior to camera operation.

Whether or not a privacy impact statement is required, users seeking to implement a video system would benefit by considering the following essential elements in the design and operation of a video system (e.g., see [17]). Any written policy should explicitly discuss:

- Why video is being collected and retained;
- Whether cameras will be covert (hidden) or overt;
- Whether there will be notice given to those in the area (i.e., with signs);
- How the images will be used;
- What analytics (i.e., automated systematic computational analysis), if any, will be applied to the video data;
- Whether attempts to identify individuals in the video data will be made systematically or on a case-by-case basis;
- What other information will be combined with the video as part of processing;
- Who is authorized to view the images and the processed data;
- How long the video will be retained under normal circumstances;
- What measures will be necessary to block or override automated deletion;
- Whether the results of analytics are stored directly with the video or stored elsewhere;
- Whether additional privileges are required to access the results of video analytics;
- What procedures will be followed in order to disclose the videos to others, both inside and outside the organization; and
- What procedures will be followed prior to public disclosure of video data.

Across the spectrum of issues outlined in the following sections, consideration should be given to minimizing any impact on privacy. Focus needs to be placed on ensuring that only public areas and conduct in those areas are the target of video observation and recording. The storage and subsequent use of data also need to address privacy concerns.

Security Issues

As with privacy, security considerations should be addressed in all aspects of creating and managing public safety video systems, as well as any systems that interact with the greater public safety video and data ecosystem. Security is critical to ensuring the availability of the video system and the integrity of its data. Inadequate security of the system will leave users unable to access critical data or to rely on the accuracy of collected data. Moreover, a lack of proper security impairs the ability of government users to ensure that data are only utilized for proper governmental purposes, and that the privacy of individuals is protected.

The provision of security must address both logical and physical realms (e.g., see [18]). The provision of security requires an understanding of vulnerability to both physical and virtual attack from both external and internal sources. For example, the U.S. Department of Defense provides guidance for designing electronic security systems, including protecting CCTV video data [19]. In every process for system operation, thought must be given to protecting components and data from compromise and improper use. As video systems grow more complex and networks grow larger, that challenge increases. The rapidly growing range of hardware and software utilized for system operation further enhances the challenge. The tasks of access control and system security are essential elements implicating a range of virtual and physical security measures. Those measures should be identified in written policies.

Security concerns with high quality video begin with the potential for unanticipated revelations regarding the scene being recorded. High-resolution recordings may contain sensitive information not immediately visible. Cameras with pan-tilt-zoom (PTZ) may be re-oriented after installation. Mobile cameras may be unintentionally taken to sensitive areas that should not be photographed.

Communications between the camera and the video analysis and storage systems should be encrypted to prevent eavesdropping and hacking. If the camera is remotely controllable, the controls should be secured to prevent unauthorized access — for example, with a complex password or with Public Key Infrastructure (PKI) certification. It may also be appropriate to use encryption to protect data at rest, either using an encrypted storage container or an encrypted video format. Encryption may also be appropriate for video that is exported to removable

storage devices. Cameras that communicate wirelessly or over the public Internet are further susceptible to jamming through wireless interference or denial-of-service attacks.

Systems that provide for monitoring, analysis, analytics and storage should similarly be secured to prevent unauthorized access. Systems that can be accessed over the Internet, such as cloud computing systems, may require additional security measures such as a physical token. Systems should have an audit trail so that staff access can be monitored. Video that is no longer needed should be securely deleted or overwritten.

Transparency Issues

The sensitive nature and scope of the data captured by video systems may cause great concern among a wide range of individuals and groups. The privacy issues outlined above give rise to substantial public attention. Even when the public goals are well documented and accepted, there is often public concern over the willingness and ability of government agencies to limit activities to stated goals and ensure matters like privacy and security of data are adequately enforced.

Transparency is both a strategic concept for policy planning and an operational concern regarding the monitoring of operations. Thus, ensuring transparency in data collection and use has two key components: commitment to system openness in the promulgation of policy; and establishment of mechanisms to ensure compliance with policy requirements. The first factor centers on the process of policy formulation and articulation. The second factor requires a strong routine of performing audits.

Openness in Policy Formulation

Addressing concerns over potential government misuse in the collection or storage of video data begins with an open democratic process for policy development. There are many ways to build a sense of openness, such as public notice and comment processes, public hearings, focus groups or other forms of civic engagement. The use of a process to develop privacy impact statements may be useful in creating a more open environment for policy development.

Whatever the mechanism of civic engagement a community might select in seeking input for its policy development, the result must be a clear set of written policies and procedures covering system operation, which are then prepared and made available to the public. These documents should clearly articulate the governmental purpose(s) for the system and the measures employed to protect privacy and afford data security. Overview information should be available to the public on the technology used for system operation, interoperability issues and the process for continuity of operation. Budgetary information should also be provided, including

the outlining of system development and operation costs (note: almost all of this information would be required by general open government statutory and ordinance requirements).

Consideration should be given for the policy to specify the responsibility of individuals and entities in the design, implementation and operation of the video data system. This includes supervisory responsibility, accountability for specific tasks and management oversight processes. Where possible, specific measures for ensuring success of policy implementation and operations should be identified.

The issue of transparency requires not only having the policies of the organization be open to the public, but also having procedures and practices in place to ensure these policies are followed. The purpose of this detailed articulation of responsibilities across the breadth of the organization is to present a clear path for assessment of accountability and audit.

Audit and Accountability

When establishing a public safety video program, agencies should consider development of an information technology (IT) audit process. Unlike a financial audit intended to monitor the agency's compliance with accounting standards, the purpose of the IT audit is to measure the program's effectiveness and to evaluate the system's internal controls to protect agency information and privacy. This operational audit concept documents programmatic compliance with written policies and procedures. With respect to video programs, an audit serves an important function beyond that of accountability. A rigorous program of internal and external audit substantially enhances the transparency of governmental operations and increases public confidence in government programs.

During the audit process, risks should be assessed and control measures modified to prevent security breaches or operations inconsistent with established policies, procedures and protocols. Those matters need to be evaluated and tested on a regular basis. Programs should have regular internal tests and performance reporting, supplemented with a periodic independent review by an external party. Careful consideration should be given to a wide variety of factors. These include whether the program's goals and objectives are being met, and program governance to ensure adequate oversight, asset security and data integrity. However, instituting only a governance structure with policies and procedures for audit is insufficient.

Common Technical Issues in Operations of Public Video systems

Common technical issues in the operation of public video systems are also part of the overarching substantive issues that must be addressed. These issues include: video data technology considerations; system interoperability; and continuity of operations (COOP).

Technology Considerations for Video Data

This section outlines considerations for the process of arriving at decisions about how to select the type of video technology. It does not address the identification of specific technology or technologies for use in any given system. An important companion to this work with respect to identifying suitable technology for use is the Digital Video Quality Handbook [3]. Also useful for developing specifications are the VQiPS User Guide [1] and interactive web tool [2].

Video System Infrastructure

As noted above, government agencies should develop a clear vision and scope for the purpose of the video system to be developed. A formal *Charter* is recommended to specify these elements, as well as the following:

- Who will be the project sponsor;
- What is the source of funding for the system;
- Who will be customers and stakeholders of the system;
- What will be the governance structure for the construction, as well as operation of the system; and
- Where will the governance structure organizationally reside.

When developing the project or portfolio of projects to develop the system, understanding the *people-oriented aspects* and *processes associated with the technology* will also be critical to ensure alignment of the technology and adoption of the system.

A plan should be developed, including a "Project Approach" document, which will outline all the elements to be considered when formulating a Project Implementation Plan and to refine the Project Scope. This should include the following (asterisks indicate steps requiring sponsor and stakeholder concurrence):

- Stakeholder assessment;
- Functional requirements*;
- Current state assessment;
- High-level solution design*;
- Development of implementation plan;
- Development, posting and communication of requests for proposals (RFPs);
- Conduct vendor evaluation & selection*;

- Planning and procurement phase close-out & lessons learned;
- Kick-off design and implementation phase of fusion project; and
- Project implementation and acceptance.

Technical Concerns (considerations for the design and procurement processes)

Once the goals for the system and scope for the project have been defined, it is recommended that a team comprised of both technical and functional stakeholders use as a benchmark other instances where a system of similar size and scope is operational. It is important that this process not be done purely within an IT organization or team. Benchmarking against another jurisdiction will allow for better understanding of lessons learned regarding technologies and approaches. It will also aid in understanding the many variables to be considered in the system design and deployment.

The following variables need to be considered in the larger goals and scope of the system context:

- Standalone system or part of a larger network or system.
- Camera locations – what is the geography/mission to be covered?
- Specifications for technical infrastructure (size, capacity, bandwidth, speed, etc.) – what will be required for the worst-case scenario to ensure quality of service?
- Video source specifications (what is required for mission vs. infrastructure?) – available bandwidth vs. video quality required; needed lighting and image definition relative to budget and mission; storage limitations vs. what is being generated (e.g., is high-definition really necessary?). Consideration should also be given to viewing capabilities relative to video captured (e.g., high definition video with only standard definition monitors or bandwidth).
- Analog (if existing) vs. digital system.
- Thermal and infrared – does this technology add value to the mission (e.g., thermal for helicopter video is useful, but not necessary for identifying suspects on the street)?
- Need to accommodate legacy or emerging technology – need to scale over time vs. one time design/build/operate approach.
- User locations – distributed vs. centralized.
- Connectivity/Backhaul availability – is there fiber available from other parties who could gain a mutual benefit from an asset-sharing scenario (e.g., providing fiber in certain areas in exchange for access to the video; providing capacity on major regional microwave or other systems)?

- Retention period for recorded video – what is the balance among length of retention periods to support operational concerns, data storage capacity and open records requests?
- Acceptable video quality and response time (e.g., eye-blink vs. seconds vs. frames per second/minute).
- Will video be actively monitored vs. recorded and made available for incident management and response?
- Number of concurrent users.
- Job tasking on the same cameras; for example, will they be used to support more than one objective?
- Analytics and automation requirements (cost of infrastructure and support relative to primary video management/content management systems).
- Extra-system video sharing (e.g., partnerships) and interoperability.
- Security (network, data center and camera) sensitivities.
- Mission criticality and acceptable outages.
- Ownership of cameras (operational decisions for user priorities and access) and content.
- Customization vs. ease of support.
- Compliance with existing IT standards.
- Ownership of technology vs. content – centralized vs. distributed, strategic/core vs. necessary for operations.
- Tolerances for proven vs. emerging technologies.
- Mobile and nomadic needs (ground, marine and air).
- Environmental considerations for mounting locations – weather conditions including frequency of lightning strikes/impeded electricity for high-elevation installs, grounding and surge protection considerations, "five-nine's" (99.999% up time) capability for wireless in rainy locations, etc., wind vs. mounting stability/safety.
- Historic District considerations for CCTV locations.

When developing a video system and beginning the procurement process, consideration should be given to starting small, using a pilot or proof of concept that will allow for learning what will best meet the needs for the mission at hand and for determining how homogenous or variable a system design will ultimately become. For instance, video systems for site security tend to be fairly homogenous with a central viewing location, with standard cameras and lighting, and with fairly straightforward video transmission capabilities (wired with some wireless in a controlled environment). In public spaces and with regard to how expansive the system's reach will ultimately become, variability and complexity will increase in proportion to those factors.

The presence of different video sources, lenses, fixed vs. PTZ, low light vs. well-lit conditions, wind/lightening/rain, obstructions, intermittently introduced radio frequency (RF) interference, construction, damage and many other factors will constantly impact the system during development, as well as operation. Also, the number of stakeholders will likely increase and thereby bring more complexity to the system.

It is recommended that objective subject matter experts provide assistance with the design, selection, build and quality assurance process. This expertise may be from one individual, a consulting firm or a large engineering firm with integration expertise. There are positive and negative implications with any of these options, so it is important to understand what will be best in a given instance. Objectivity is most important in identifying the correct technology for the mission and in avoiding solutions that may prove limiting in the future.

A multi-disciplined team that represents the points-of-view of both technology and function will then need to develop the list of basic components that will be procured and implemented by the system. The primary components consist of the following (some elements may already exist, but are then repurposed or leveraged, while other elements will be purchased/implemented):

- **Video Transport Network** – This is the fiber or wireless network to connect components. This may be within one structure or between many locations. Existing infrastructure or standards should be considered when making this decision. Wireless technologies are typically considered when fiber is not available. When considering these products, it is important to understand your operational RF spectrum. For example, 4.9 GHz is the current public safety band and requires a license. The criteria regarding what needs to be licensed (ranges vs. specific locations) vary depending on the situation, so it is important to consult your local FCC coordinator or the FCC itself. It is important to note that resellers of licensed equipment are not responsible for making certain you know about the need to license your installation or any compliance issues. Other unlicensed bands are available. Often a mix of several is warranted to avoid having devices conflict with one another for space (such as the case in closely spaced mesh locations in a dense downtown environment). Also, bandwidth and distance are key considerations when selecting a product. It is highly recommended that an RF or wireless subject matter expert be engaged to review needs and choices and to provide objective expertise regarding this choice.
- **Video Management System (VMS)** – This term can be broadly used pertaining to various approaches to building this infrastructure. It is generally comprised of a server for processing content and supporting user's requirements for viewing, as well as recording and storage needs. These can be built as "Best of Breed" IT systems consisting

of readily available best of breed components. At the other end of the spectrum, they can be a "black box" solution that is a pre-configured VMS on a server pre-programmed and implemented specifically to a customer's needs. The considerations given to how the system will be structured are cost, reliability of the products, reputation/viability and longevity of vendors for service after the sale, and adherence to a proprietary relationship/contract vs. the ability to replace/upgrade various components as technology changes. The "black box" type of systems can be easier to implement, but may allow for less customization or growth, or the ability to change vendors as other products deemed a better fit emerge over time.

In addition to the technical elements, there are several additional key aspects of the system above:

- Server environment;
- Software;
- Storage;
- Cameras;
- Wireless systems;
- Mobile systems (portable video systems – trailers, rapid-deployment, helicopter downlink, etc.);
- Analytics and automation; and
- Reporting and system optimization & monitoring.

It is important to have a solid description, functional requirements and scope of work for the evaluation and procurement of these elements. Depending on the products, the solutions will be some combination of hardware and software. Additionally, a criteria matrix for what is being evaluated should be developed, and a team of evaluators should provide input. Depending on the solution being considered for purchase, user demonstrations and scoring may also be part of these criteria to evaluate which best meets their requirements. Typical criteria are:

- Vendor/product references and qualifications in projects of similar size and scope;
- Vendor reputation and reliability in the marketplace;
- Vendor installer experience with the same product;
- Cost;
- Availability of local support;
- Recurring costs after implementation;
- Complexity to support;
- Warranty;
- Adherence to existing agency/company standards;

- Technical solution vs. functional requirements;
- User experience; and
- Ability to train internal resources to support.

If the procurement is to be made by a governmental agency, the existence of purchasing contracts or cooperatives may be another major consideration in the selection process. If RFPs or bid processes are required, it is recommended to consider a high-technology best value approach for the procurement as opposed to a lowest-bid/winning bidder approach. The latter may not adequately take into account the proposed solution quality or vendor reputation. Best value provides for the ability to show that, while the cost may be higher, the overall return on investment (ROI) or highest value will be the best selection. This usually is evident in selection factors addressing quality, minimization of outages and down time, supportability, flexibility, ability to customize, scalability, non-proprietary in nature, lower future support costs, and so on. A facilitator may moderate the evaluation process, including administering any system demonstrations and scoring, while a procurement officer should conduct the actual vendor selection and award. This should increase alignment of the final solution to the original goals and objectives.

Interoperability for Video Data Sharing

Considering interoperability among system components and with other systems is very important when designing and implementing a Public Safety Video System. Although a video system may be established using the best available standards and practices for the type of system being built, there may be multiple components from different vendors being used as building blocks in the overall system. When designing the system, the performance and interoperability of the entire end-to-end video system should be tested, as well as when new components are used to build out the reach and capability of the video system.

Each given product may have features that are proprietary and may not necessarily facilitate interoperability across system components. Making certain that different components work together is a system engineering problem and one that must be addressed by the video system owner.

The public safety needs require that the quality of the video be taken into account all the way from the source to the end user. Extensibility and scalability of the vendors' products are also important because the video system may be expanded over time, so obsolescence needs to be minimized to save future costs. Including interoperability in the overall video system design will likely drive open-architecture or interoperability requirements in the procurement specifications to the vendor. The policy for interoperability should include considerations for

connecting with and leveraging existing infrastructure (including legacy video systems), as well as emerging technologies.

Another key consideration with regard to interoperability will be the requirement to partner or share video with other jurisdictions or agencies. The video system owner should develop and approve a sound network architecture and integration approach that complies with standards and security requirements, as well as addresses other areas of concern. This model can then be repeated and validated with the various partner agencies. A stable platform of proven, open, scalable and reliable products will facilitate the ability to develop video-sharing partnerships. The more closed or proprietary a system, the less possible this becomes (without spending more time and money on custom solutions or additional vendor products).

One approach to achieving interoperability involves having the agencies that share video purchase all of their equipment and software from the same or compatible vendors. This was the approach taken by the Hybrid Analog/Digital Management System [20] established in 1998 by local, county and state agencies in the Silicon Valley area of California to monitor traffic and public safety. However, because different jurisdictions often have different funding and budget schedules, policies and processes, requiring each agency to use the same vendor technology is generally not practical unless the entire region is collectively and simultaneously upgrading their video technology. Another approach was developed in the national capital region (NCR) of Washington, D.C., with the intention of avoiding additional costs that might be incurred by requiring those sharing video to replace components of their current video infrastructure [21]. This approach instead allows each agency to retain its own technology, while adding an "integration layer" that allows these disparate video systems to share video. This integration layer contains hardware/software/networking components in the form of three or more small Linux computers that normalize the shared video to a format that can be viewed in almost any browser or application.

Continuity of Operation (COOP)

Public safety video programs have increasingly become essential functions of meeting an agency's mission. Resilient organizations develop the capability to perform these functions on a continual basis even during emergency situations, cyber-attacks, power outages or a myriad of other disruptive incidents. Assuring COOP requires planning and coordination among agency personnel and outside vendors providing program support. Agencies should assess their risk and develop measures to prevent and control disruptions, as well as to quickly restore processes and systems after a disruptive event has occurred. When developing the agency's COOP plan, it is important to determine what functions of the public safety video program are mission critical. Establishing recovery time objectives not only will set expectations for the level of service to be provided, but also serves as the basis for mapping recovery processes and

capabilities. During the planning process, agencies should engage key stakeholders including partnering agencies, vendors, cloud services, etc. This will help ensure that roles, responsibilities and capabilities are clearly defined in advance.

ISSUE ANALYSIS

Beyond the above overarching issues that permeate almost every aspect of any government video system, policy makers identified a number of other issues related to the development of their video programs. Those issue areas are:

1) Sighting and location;
2) Access and use, including search;
3) Source considerations;
4) Notice considerations;
5) Monitoring, analysis and analytic applications;
6) Retention of data;
7) Dissemination of data; and
8) Governance issues.

Issue Analysis Format

To ensure consistency, the VQiPS Policy Subcommittee agreed on a format for discussion of each of the issues listed above. As mentioned earlier, the underlying goal of the Policy Subcommittee was not to recommend a specific policy solution, but instead to provide a common framework for analysis and guideline for discussion and deliberation on the issue. The following is an outline of that format for deliberation on each issue:

Background and Description provide the user with a context for the issue's importance. It attempts to pull together the parameters of the issue and outline where that issue fits in the larger context of video system operation.

Assumptions identify some of the commonly accepted understandings that underlie most governmental video programs. If those assumptions are not accepted by a jurisdiction that is considering the video system, caution should be exercised with respect to issue guidance in that section. This is not to say that this section therefore would be without value, only that differing assumptions may affect the applicability of the issue analysis.

Strategic Objectives address major issues of policy direction to achieve a program's or project's aims. The focus of Strategic Objectives is to define approaches to issues that are essential to the accomplishment of a program or project. Strategic objectives provide guidance for operational and technical measures that ensure achievement of defined policy goals.

Operational Measures are derived from Strategic Objectives and offer a defined path for achieving those Strategic Objectives. Concrete steps addressing the broad concerns of the Strategic Objectives characterize Operational Measures. Operational Measures provide the framework for written protocols or procedures implemented by organizations in order to manage a program and project.

Technical Measures are supporting technology procedures and directives that combine with Operational Measures to meet Strategic Objectives. These measures govern issues like hardware and software selection, maintenance and administrative requirements, and matters of technology policy required for proper system function.

Stakeholders include attempts to outline those internal and external individuals, organizations or agencies that are commonly involved in assessing a given issue. Of course, the stakeholder analysis will certainly vary depending on any given jurisdiction's structure. However, this analysis should serve as a starting point for identifying interested parties. It should serve as a catalyst for analysis by policy makers regarding who should be sought to provide input to the decision-making process.

Impacts result from the identification of the effects that policy decisions on one issue will have on other issues and other considerations for system operations.

Special Considerations are additional policy considerations that should be addressed by policy makers.

Issue Discussions

The following discussions are the result of the application of the analysis framework mentioned above to each of the issues identified by the Policy Subcommittee.

1. Sighting and Location Considerations

Background and Description:

Sighting refers to the camera's "sight" or what the camera can see (e.g., field of view, level of zoom, lighting, obstructions and elevation). The location of the camera typically is related to the purpose of the camera, especially when designing new installations, as opposed to simply taking advantage of a fortuitous mounting location. The order of deciding sighting versus location can change depending on the type of system being built and the boundaries or restrictions affecting the effort. For instance, if a municipality owns traffic signals and pays for the power to support them, this is a location that can readily address a mission, such as obtaining video coverage of a particular geography. Once those criteria are determined to be the mechanism by which the city would gain coverage, they would then determine the best position for video sources (sighting), as well as the best type of camera to optimize coverage of

particular aspects of the area. Depending on the mission, the individual or team determining sighting and location will look at how to optimize the ability for that video source to address as many objectives as possible (e.g., critical Infrastructure protection, egress and ingress, parks vs. roadway, rail and perimeter protection, dignitary protection, etc.).

Another common sighting consideration is separation: how far apart to place the cameras. This decision may have to consider spacing and density of buildings, terrain and camera uses involving simultaneous job tasking for operators (e.g., monitoring traffic conditions, as well as security of government property). If natural topography or structures will block the view or the ability to track an incident from one video source to another, then the camera density may need to increase. This may also be a function of the capability of the cameras being utilized. For example, if the cameras are fixed, there may be a need to place multiple cameras in a location to provide different views. In contrast, a single PTZ camera might be able to cover multiple directions. A fixed, very high-resolution camera might also provide sufficient detail to allow operators to perform digital searches, such as zooming to specific areas, while continuing to monitor the wider field of view.

Sighting may also involve a variety of different information requirements. If personnel need to address differing concerns like traffic management, known threats in an area or general public safety management, more cameras may be required to prevent users from competing over resources. This multiple purpose requirement might also affect the type of equipment used (e.g., PTZ versus fixed versus high definition) as a way to solve this problem.

Another factor affecting sighting is the manner in which cameras are connected. Wireless connections and consequent bandwidth considerations will affect the quality level of the video that can be delivered into the system. Additionally, wireless signals will suffer from interference from other radio sources (known and unknown) in the area depending on the frequencies and channels available in the area. Employing qualified subject matter expert consultation when determining source locations and field of view is very important. An example scenario would be that the police nominate camera locations due to crime statistics. Before installing the cameras, one has to consider sighting (e.g., does the camera field of view invade privacy?) and location (access to power and data transmission). Funding (both the amount and who funds it) is also a factor in deciding on location and sighting. Examples of funding factors include: higher implementation costs when considering one location over another; recurring cost associated with a location; or the funding source (agency or individual interest) may have stipulations associated with the mission for the video installation.

If a particular sight or field of view will involve the use of analytics (e.g., identification of left-behind packages, crowds gathering or dispersing, change in speed of a vehicle relative to

others, etc.), then sighting may drive certain decisions in camera use. In general, fixed cameras are necessary for the successful application of analytics. In instances where users need to change the field of view and direction, PTZ cameras would be required. In situations where location and sight cannot be known in advance, then mobile video sources would be required (see section on Sources Considerations).

Some jurisdictions require a privacy impact assessment be performed in conjunction with camera location and sighting activities. This is primarily the case where video sources will be in residential areas or areas of private commercial concerns. For instance, public safety cameras in intersections with mixed land use (major thoroughfare with some residential use in the area) may need to utilize masking technologies. In these instances in particular, sighting of the camera needs to carefully consider privacy concerns. In all instances, federal, state and local legislation and precedence need to be considered. In general, the ruling by the U.S. Supreme Court [10] that there is no reasonable expectation of privacy for activity in a public space has been the overriding guidance for sighting decisions, but legal counsel should be consulted in each jurisdiction.

One final issue with respect to sighting concerns the hiding or masking of camera locations. Some public safety implementations have utilized tactics where camera locations are "advertised" with agency logos and colored lights to bring attention to the fact that the agency is watching an area. Conversely, in other situations, implementers have taken a more covert approach. The issue will be addressed more comprehensively in the section on Notice Considerations.

Camera location and sighting vary based on the nature of the camera. Camera position can be permanent, temporary or mobile. Cameras may be established in a fixed network, which can then be mapped. When there are changes in use or geographic features of an area, those cameras can be relocated or augmented by temporary camera placements. For example, cameras covering an area like a street or sidewalk may have to be moved or supplemented when construction work blocks or changes views. When there is a large event or activity planned, video observation can be augmented by the placement of temporary cameras to enhance observation. In contrast to temporary placements, mobile cameras are used to cover areas from platforms like vehicles. These types of platforms, particularly those used by jurisdictions in connection with activities like reading license plates, require more continuous monitoring from the perspective of governmental purpose and privacy concerns because their field of view is constantly changing.

Assumptions:

When making sighting and location decisions, jurisdictions should be aware of the following assumptions:

- There may be legislation in a given jurisdiction that would affect decisions regarding location and sighting. This needs to be investigated at the start of a program to determine boundaries or approval processes required.
- Memoranda of Understanding (MOUs) or Interlocal Agreements may be necessary when gaining permission to mount cameras on properties owned by other entities.
- Connectivity, power and backhaul considerations will have a considerable impact on location choices.
- The sighting of cameras will be on public areas where the conduct and activities to be observed do not give rise to a legitimate expectation of privacy.

Strategic Objectives:

A governing body or individual needs to be in place to set guiding principles and direction for selecting camera locations and determining sighting. Consistency with overall objectives and goals of the public safety purpose of the camera system should be a principal driver for location and sighting of cameras. Once those guidelines are set, then a current state assessment of assets that can be leveraged for location and sighting will be useful in understanding how best to move forward.

Considerations such as ownership of locations for camera deployment facilitate implementation. Where locations are not under the organization's control, MOUs will typically be required. The same is true for supporting power and connectivity issues (fiber or wireless antennas). Creating alliances among coordinated government departments and agencies may further facilitate sharing assets to support particular locations. An example would be getting access to fiber in traffic and rail corridors from transit or public works organizations to support backhaul for video locations. In exchange, those organizations could be given access to view video sources within range of their operations. Another example is gaining access to major microwave transmission systems around a municipality to extend system reach, with the microwave system owner being given access to fiber when there is overlap in their project missions. Backhaul is an important contingency to determining what locations can be implemented in a system.

When selecting camera-mounting locations, considerations need to be given to public perception, aesthetics, and cultural, historic and environmental sensitivities. Executive management should work proactively with the local media and public representatives (e.g., elected officials) to address public perceptions of the video surveillance initiative. In the cases of grant funding, many funding agencies will require an Environmental and Historic

Preservation review to verify installations will not have a negative impact on a cultural/historic structure, the environment or public well-being. This process will add time and possibly cost to an initiative.

Operational Measures:

When identifying locations that can be used to provide video coverage for a particular area, several factors should be considered that affect the ongoing operation of the system:

- Camera sightings and locations need to be aligned to the system purpose and Concept of Operations (CONOPS). Cameras must be capable of meeting the organization's operational needs.
- Camera location and sighting must also be consistent with legitimate privacy concerns of individuals and groups.
- Camera location needs to account for the legal authority of the jurisdiction to place a camera in the location, establish connectivity, provide power, and conduct service and repairs on the equipment. Where necessary, MOUs, easements and other agreements need to be prepared to meet these requirements.
- Camera survivability from the elements, accidents and vandalism is an important consideration. Video sources and support infrastructure in exterior locations need to be rated to withstand heat, cold and humidity for that location. Depending on the area, average rainfall and intensity of rainfall may affect wireless capabilities. Painting of housings for cameras is sometimes required by a hosting location, but this can affect the operation of a camera due to heat absorption (e.g., darker colors), and may void the camera warranty (depending on the manufacturer).
- Consideration of location should account for support and maintenance of the locations selected, taking into account support resources available to the agency or entity (e.g., bucket trucks, existing security infrastructure, maintenance personnel) and accessibility of the location (e.g., ladder required to mount a 20-foot rooftop parapet wall vs. immediate access via penthouse; needing to coordinate with property owners for timely access). In the case of wireless cameras, the locations of antennas will have an impact on operational concerns. Antenna locations may impact the quality of the video being transmitted or recorded. Processes need to be in place to check video sighting to ensure that cameras continue to provide and capture the field of view intended.
- If a camera or a wireless connectivity antenna is to be mounted on a tower, structural analyses (related to weight or wind loading) and leases may be required prior to mounting this equipment. Additionally, depending on geography, lightning and wind may have a major impact on the camera operation at those locations. Tower climbs are expensive and often have to be planned well in advance. If such locations are required, it will be important to have a support contract in place that provides for a certain

number of replacement units and tower climbs that can be readily used (e.g., having the purchase order already in place). If locations are selected in areas of growth or redevelopment, construction plans may alter the camera sighting or the camera may become disconnected or obscured. If this becomes an issue, then there are cost considerations for modifying designs over time.

Technical Measures:

The following technical concerns should be addressed:

- Implementation is facilitated when an entity specifies a select set of equipment makes/models or types to be utilized in a system. Also useful is a specified standard for when the marketplace will be re-evaluated to determine whether upgrades or changes are warranted. This simplifies ongoing support because technical resources can become proficient in those platforms, and because break/fix inventories can be maintained in those select devices.
- Standard configuration of devices needs to be determined so that sources can be pre-configured in that standard prior to being installed.
- When cameras are being deployed on a wireless mesh, users should consider testing the solutions before fielding them. For example, the mesh could be staged in a warehouse environment with a connection to the network to ensure all nodes are configured properly and would come online when installed in the field. In conjunction with bench testing of new sources during the pre-install configuration process, this will eliminate lengthy trouble-shooting that would occur after the sources are installed (particularly in hard-to-reach locations like traffic signals or rooftops). Installers should coordinate the quality assurance (QA) of the installations from the desktop prior to leaving the site location to minimize delays or costs associated with revisiting a location.
- A predetermined IP schema should be designed at the beginning of any video project. Location will play a major role in that schema, including how the system is intended to grow over time to allow for additional IP addresses to be available in a given sub-net. For instance, if IP super- and sub-nets will be allocated first by geography and then by device type, the master plan should be prepared in advance and IP addresses allocated to installers according to that master plan. The installers should then provide information regarding the location where a device was installed to update the IP master list in order to track allocation.
- The system design should allow for all components on an IP-based network to use Simple Network Management Protocol (SNMP) technology to allow the devices to be managed remotely on a network using automatic network management tools. Many monitoring tools only indicate whether a connection to a device still exists. Enclosures and housings containing network switches need to be readily accessible to persons

responsible for troubleshooting activities in order to allow for a quick evaluation as to the nature of a camera outage (power, camera, communications links, etc.).

- Where possible, fiber connectivity should be the preferred method of technology because fiber allows cameras to remain functional during heavy storms, provides protection for connectivity and results in better bandwidth for video sources. If wireless connectivity (i.e., point to point, wireless mesh, Gig link) is the only option due to availability or budgets, then a rating of five-nine's should be considered in areas where rainfall is frequent and may be heavy. These ratings indicate the amount of time that a device is expected to operate in a given geography. Radio Frequency (RF) engineers can calculate these numbers depending on location.
- RF conditions must be addressed. A thorough understanding of the RF conditions in a given area is important to the quality of video achieved in a given location. A qualified RF engineer can determine this and make recommendations as to the frequency to be used in the wireless infrastructure at the location. The 4.9 GHz frequency is provided for public safety uses and is also available for use by traffic agencies. Because the user community allowed to use this frequency is more limited, doing so also will allow for fewer channels at the necessary bandwidth than some other options. Balancing all these considerations will be important in a given location. To the extent possible, it is advisable to work closely with other public safety agencies, as well as those known to be utilizing wireless technologies to minimize interference between systems. This may be a challenge due to competing interests and because some parties will often want to avoid sharing their plans.
- There needs to be an understanding of how your wireless system might interfere with others in the area. For instance, if there is close spacing of a wireless mesh camera system in a densely populated high-rise area, then an agency's own radios may interfere with one another. Tri-polarity antennas can help with this, as well as the ability to use multiple bands and channels within those bands. Additionally, a helicopter downlink system might interfere with ground-based or mobile unit (land or marine) wireless locations.
- Depending upon the mission criticality of a video location, Uninterrupted Power Supply (UPS) capabilities need to be considered. The circuits for the building itself may already have UPS capabilities in place. If not, local UPS capability at the switch or device may be necessary. Additionally, surge and lightning protection need to be addressed. Some buildings have "dirty power" that requires the protection of sensitive electronics. While no equipment can be protected from a direct lightning strike, Lightening Protection Units (LPUs) are available to be placed in line to prevent energy from electrical storms from traveling up or down a cable and damaging the electronics. Consideration should be given in the technical design as to where the LPUs will be placed in tower

applications. These devices will fail more frequently than a radio that is reinforced to withstand this impedance and could result in costs related to tower climbs. At a minimum, an LPU should be placed at the base of the tower to protect the equipment in a tower support building. Newer tower radios place the electronics on the tower itself, as opposed to large radome antennas being placed on a tower and the radio being placed in the support building. These types of systems are more expensive to purchase, but may be cheaper to maintain over the long haul given the electrical storm/tower dilemma.

- If cameras are located or sighted within areas that have the potential to involve privacy concerns, then automated solutions like image masking or virtual or physical restriction on camera operation should be considered to ensure privacy.

Stakeholders:

Selection of sighting and location requires input and collaboration among a wide array of stakeholders, with each having an interest in the program outcomes and oversight. Agencies developing video programs should consider engaging the following groups:

Internal

- Executive sponsorship (to set direction, but also assist in negotiating with location owners or owners of facilities used for source locations; manage any media or public concerns about the initiative);
- Departmental management (functional and technical);
- Operational users (first responders, criminal/civil investigators, transportation, public works, etc.); and
- Technical implementers (information technology, procurement, project managers, facilities management, transportation engineers, permitting and planning).

External

- Property owners;
- Utilities and public works (for support infrastructure);
- Regional public safety agencies (traffic management; 911 call centers; local, county and state governmental agencies; flood/water districts; critical infrastructure agencies and districts);
- Commercial entities with public safety concerns (stadiums & convention centers, ports, universities, airports, medical centers, stadiums, convention centers);
- Community partners (e.g., management districts, chambers, business improvement districts, neighborhood associations, etc.);
- Media (managing public perception and concerns when necessary; proactively informing the public of the intent of the system); and

- General public (balancing program goals with privacy issues; managing expectations).

Impacts:
Access to quality video from the right location at the right time is key to the success of the system. For first responders and other public safety personnel, relevant functionality and improved results (force multiplier, effort reduction and collaboration) is what will determine their willingness to incorporate the use of a system in day-to-day operations. Understanding the functional and operational requirements, known threats and hot spots, and event types and timing will be key to properly selecting locations and determining sighting requirements for a system. While it is impossible to anticipate the location and timing of every incident, taking the best knowledge and assumptions into account will increase the likelihood that a video program will capture an incident, either recorded or in progress.

Special Consideration of Sighting and Location—Environmental, Historic Preservation and Aesthetic Concerns:
The placement of camera sensors around a city, campus or building can raise environmental, historic preservation and aesthetic concerns. These concerns can have implications for system design, cost and operation. They can also affect issues like community support. Some examples follow that illustrate these concerns.

For example, in an attempt to make street cameras blend more closely with the design of the street lighting system, a jurisdiction determined that camera housings would have to be black—the same color as the light poles and traffic signal lights on which they were mounted. This decision on the color of camera housing had significant impact on the design and cost of housings that were designed to be white to minimize the effects of heat on camera operation. Alteration of manufacture design may serve to achieve aesthetic objectives, but those decisions are often not without cost.

A second example involves the placement of cameras on structures of iconic, historical or artistic value. In this case, a jurisdiction was looking to enhance coverage of a public park and therefore placed cameras atop the highest structure, which happened to be a piece of artistic design. The reaction of the media and the general public was swift and highly unfavorable. The cameras were quickly removed. The important point is that placement of cameras in and on iconic structures should be done very carefully and with consideration of public sentiment.

Another example would involve the placement of cameras on buildings listed in the National Register of Historic Places (http://www.nps.gov/nr/). Height of rooftop antennas and color of

equipment could become an issue. Federal, state and local historic preservation standards should be considered and are usually readily available.

Even in structures that are not iconic, there should be concern over the change that obvious camera deployments can make to the look and feel of a space. In some circumstances, obvious camera deployment may enhance the space by providing a greater sense of security. An example of this is the practice in some police jurisdictions of placing blue lights on cameras in high crime areas. In other instances, overuse of cameras in a confined space or area may create an oppressive feeling.

To be sure, any judgment of aesthetic correctness will vary from person to person and community to community. The key is to be sensitive to those issues and responsive to any concerns of those involved.

2. Access and Use (Real-Time and Forensic) of Video Systems and Data

Background and Description:

The promise of video to aid in a range of public safety operations and other governmental functions is something that is being increasingly embraced in all levels of government. As noted in the earlier section on Public Safety Goals, video use post-9/11 has greatly expanded, both in real time and forensically, and is now found in jurisdictions large and small.

At the same time that video system usage is expanding, there is a growing awareness on the part of the public of the scope and power of these systems. Government actions making large-scale observations of public conduct and digital file maintenance of that conduct have raised questions about possible interference with civil liberties. Video programs in particular have raised concerns about threats to personal privacy. Concerns are raised not only by the use of images, but also by the use of metadata captured along with those images. Metadata is the set of information about the data that includes the file structure and basic descriptive information (e.g., location, time). Using metadata can make it easier to search, sort and retrieve the actual data.

Addressing legitimate privacy and civil liberties concerns requires commitment to ensuring achievement of two important results: first, that information gathered is utilized only for approved public purposes; and second, that information is properly safeguarded. Systems must contain measures that ensure proper use of video systems by authorized personnel and protect against unauthorized system use or release of data. This relates to the overarching substantive concerns identified earlier. Transparency in the creation and execution of those measures is important in maintaining public confidence.

With respect to access and use, it may be helpful to consider differing aspects of video and video data that are related to the temporal factors associated with real-time versus forensic use. Different rules might be applied with respect to access and use based on temporal concerns. In real-time use, the concerns focus on how the system is being operated. Questions can arise with issues like turning cameras on and off, and where cameras are aimed and focused, particularly in the case of PTZ cameras that operators can adjust. There are both real-time and forensic concerns about the review of data collected by the cameras. The rules for access and use for those activities can, and often do, differ based on considerations of time and purpose. Because another set of issues arise from the actual operation of the equipment itself as opposed to the data collected, those access and use issues are addressed under the considerations for real-time access and use.

Assumptions:

The following are important assumptions for access and use:

- The groups of individuals with a need for real-time access and forensic access, depending on the size of the agency, may involve overlapping or completely separate populations of individuals. For example, a small department may have police officers who investigate crimes also working to monitor cameras in real-time, whereas a larger department may have investigations only conducted by detectives. As another example, police, fire and emergency medical services (EMS) may be performing real-time monitoring for a large-scale event, but only the police would investigate any crimes that occur at the event.
- The purposes for forensic and real-time use of data may involve overlapping or completely separate needs (e.g., managing traffic; research for a criminal proceeding).
- Images, their associated metadata and forensic data may have different use and access requirements.
- The increased time over which forensic investigation is generally conducted allows for greater review and supervisory input for decisions on who can access data and for what purposes.
- Video systems operated by a given agency should have sufficient technical capability to establish permissions and controls around determinations made with respect to those who can access cameras and data.
- Permissions and controls can be configured to require approvals for access, which can be required both for individuals and for specific purposes.
- Technology systems can be employed to document compliance with permission and control policies.

- Most access and use decisions will be decided by an organization based on operational need consistent with governmental purpose.
- Having transparent policies for access and use, and the execution of those policies, will increase public confidence and mitigate privacy concerns.
- Internal and external audits are important parts of a program of transparency.
- Legislative bodies and courts may place requirements on access and use.

Strategic Objectives:

An agency must have a comprehensive written policy governing the terms and conditions for data access and use. This policy should be predicated on the need for the individual to access the system and to use the data he or she is seeking. That policy must recognize the differing needs for: control over access and use of collection modalities; access and use of real-time and near real-time data; and access and use regarding stored or archived data. Rules for governing access and use should be tailored to ensure that governmental purpose is effectuated, privacy is protected, and the system is safeguarded against unauthorized access or use. Owing largely to time issues and differing needs for information in real time as opposed to forensic use, it might be beneficial to structure access and use policy to reflect those realities. Some flexibility may be appropriate to ensure appropriate information access in real time, especially in emergency situations. However, rules for governing access and use of stored and archived data should be more restrictive. Whatever the decision on policies and protocols for access and use, measures should be put in place to rigorously enforce those policies and protocols. The policy should outline the legal, operational and technical implications of access and use.

Operational Measures:

The following are operational considerations regarding access and use of video systems. Consistent with the suggestion above, real-time and forensic uses are distinguished.

For real-time access and use (including manipulation of the video data collection system itself), the following matters need to be addressed by operational policy:

- Establishment of a process for providing access to cameras and real-time data (who, what, when, where, why and how), a system for supervisory oversight and system for activity reporting.
- Establishment of a process to ensure that users are properly credentialed.
- Issuance of specific user identification and imposition of security measures (e.g., password or biometric systems) so that user access can be authenticated and tracked, and user activities can be tracked and monitored (ultimately showing who the user was and exactly what they were viewing).
- Development of a video CONOPS to set priority access to video feeds.

- Requirements-based hierarchy of controls and permissions.
- Mechanism in place to adjust permissions based on the situation.
- Creation of protocols for granting and denying access to cameras.
- Creation of the ability to provide real-time access to “boots on the ground” responders.
- Establishment of recording permissions/limitations.
- Establishment of controls to limit export and dissemination of live or recorded digital media content (DMC).
- Establishment of training programs to ensure technical proficiency and a clear understanding of user system permissions.
- Development of an internal and external audit regimen to monitor compliance with access and use rules.
- Establishment of discipline and re-training programs for individuals identified as non-compliant with policies and protocols.

For forensic access and use, the following matters need to be addressed by operational policy:

- Establishment of a process for providing access to cameras and forensic data (who, what, when, where, why and how), a system for supervisory oversight and system for activity reporting.
- Establishment of a process to ensure that users are properly credentialed.
- Issuance of specific user identification and imposition of security measures (e.g., password or biometric systems) so that user access can be authenticated and tracked, and user activities can be tracked and monitored (ultimately showing who the user was and exactly what they were viewing).
- Establishment of a system of approvals and permissions for access to stored video data.
- Establishment of a system of approvals and permissions for actions with respect to stored data including: copying, altering, removing or destroying stored data.
- Development of protocols to ensure evidentiary usage consistent with jurisdictional requirements.
- Development of a schema to ensure user access does not interfere with established preservation practices and destruction in accordance with established retention schedules.
- Establishment of a notification system so that interested users can take necessary steps to preserve needed data before destruction.
- Establishment of training programs to ensure technical proficiency and a clear understanding of user system permissions.

- Development of an internal and external audit regimen to monitor compliance with access and use rules.
- Establishment of discipline and re-training programs for individuals identified as non-compliant with policies and protocols.

Technical Measures:

The following are technical considerations regarding access and use of video systems. Consistent with the suggestion above, real-time and forensic uses are distinguished.

For real-time access and use (including manipulation of the video data collection system itself), the following matters need to be addressed by operational policy:

- The system should be architected so it can be managed through a system of permissions and controls with respect to access and use.
- The system should be architected so that users can be properly identified and their activities can be tracked and monitored.
- The system should be developed in a fashion to ensure that all video feeds, including those provided by wireless devices, can be accessible in real time.
- The system should be developed in a fashion to ensure users have the ability to send and receive video data from any geographical location to whomever needs to see it.
- With respect to the development of the video system itself, focus needs to be placed on availability, reliability and survivability of collection systems and image data.

For forensic access and use (including manipulation of the video data collection system itself), the following matters need to be addressed by operational policy:

- The system should be architected so it can be managed through a system of permissions and controls with respect to access and use.
- The system should be architected so that users can be properly identified and their activities can be tracked and monitored.
- Where a system of supervisory approvals and reasons for access are required to be specified, the system should be able to track and report compliance with those measures *before* access is granted.
- The system should be developed in a fashion so that controls are in place to protect against unauthorized access, copying, alteration or destruction of stored data.
- The system should be developed with safeguards that ensure backup and preservation of data.

- With respect to the development of the video storage system itself, focus should be placed on availability, reliability and survivability of collection systems and image data.

Stakeholders:

Stakeholders include individuals within a jurisdiction's governmental structure, as well as numerous external constituencies who may want to access video data. Stakeholder groups include:

Internal

- Policymakers;
- Operational users (first responders, criminal/civil investigators, transportation, public works); and
- Technical implementers (information technology, procurement).

External

- Policymakers and records supervising agencies (e.g., state legislatures, state/local archivists);
- Operational users (first responders, criminal/civil investigators, transportation, public works);
- Legal counsel (to review policy to ensure compliance with legal requirements on access and use);
- External data recipients (e.g., judges, prosecutors, public defenders and private criminal and civil attorneys — who need assurance that data is not altered or compromised);
- General public (concerned about data use and privacy); and
- Advocacy groups concerned about data use and privacy (e.g., Electronic Privacy Information Center (EPIC), American Civil Liberties Union (ACLU)).

Impacts:

Determinations on access and use have impact across all video system elements and underpin all aspects of system operation. In addition to shaping the operation of system, decisions on access and use can also shape the type of technology a system may utilize and how a system is architected. These impacts begin with the actual collection of the data itself, when to turn cameras on or off, record or not record, or control focus and direction (i.e., PTZ) of cameras. These real-time concerns need to be addressed along with the real-time imagery and metadata the cameras generate.

Controls on access and use are key to ensuring that the overarching goals of governmental purpose, privacy protection and system security are achieved. Decisions (including: who can use the system; what data they can capture or access; and under what circumstances) need to be

clearly documented in policy and then reinforced through a series of other measures. These measures include supervisory structures, systems of oversight and audit, and automated permissions and controls built into the technology supporting the system.

In establishing and implementing technologies on use, consideration should be given to temporal concerns and the need for flexibility in emergency circumstances. The rules on access need to ensure that organizations have the ability to access and use data, particularly in real time. Conversely, as the data become older, there should be increasing review and scrutiny for access and use. The same scrutiny should apply as the scope of data review increases or when there is an attempt to create files or dossiers of individualized data.

Special Consideration for Access and Use — Categorization of Video Data Content:
Categorization of content refers to the organization and "labeling" of video content to facilitate and expedite the use of that video for the designated mission of the system. The development of this information system architecture needs to be aligned with the underlying governmental purpose for which the system was established. It should address both the images to be observed, and the images to be collected and recorded. This categorization process concerns not only images, but also the underlying metadata that is now captured by digital systems. All data that a video system touches should be categorized.

Operators need to ensure that only data fitting into identified categories is collected, recorded or used. The development and application of these categories should be determined by a group that includes the stakeholders who will ultimately utilize the video content for specified use cases and in accordance with standards, Standard Operating Procedures (SOPs), legal guidelines and technical functional requirements.

Rules for the use of the video system and content, and therefore the categories implemented in the system, may be guided by the source of funding used to develop the system (e.g., stakeholder interests, or grant requirements and restrictions). This may also affect the ability to share that video (and therefore categories are applied to easily separate security sensitive video content). The policy developed for categorization of content should clearly define these requirements and include what is and is not acceptable to ensure proper use of the system and adherence to legal requirements. An example would be determining at what point the use categorization of the video changes from generic situational awareness to Criminal Justice Information Services (CJIS) regulated content (i.e., data that may be used for evidence in connection with criminal proceedings or other criminal justice processes like intelligence gathering). This may occur though manual investigative processes or through the use of

analytics and other automated tools. For example, once the analytic tools in a system begin to identify a potential individual and categorize content based on that identity, this might require that these data now be maintained under a regimen such as CJIS technical guidelines for security.

Categories typically are warranted for use with automated video analytics tools (live video), but may also be used for video content analysis (recorded video). Categories related to these applications can assist in situational awareness and incident response where they provide real-time detection and alerts, and thereby aid in defining events and scenarios when those events are detected.

Carefully selected categorization may also be useful in forensic analysis and search of DMC, where the categories may greatly reduce the amount of time and personnel required to search recorded video to pinpoint specific video frames (e.g., [7]). Examples of categories are:

- Target type – people, vehicles, static objects;
- Event type – moving, stationary, crossing a line, occupancy, crowding;
- Filter by color;
- Filter by size;
- Filter by defined time ranges;
- Search on selected cameras or group of cameras; and
- Search for similar targets – Once a target is observed, a simple search can be conducted to locate additional appearances of the same or similar target in the recorded video.

Categories can also aid in analyzing video footage to generate statistical reports from data collected within the video. Examples of uses of these types of categories include:

- Vehicle traffic analysis;
- Behavior analysis (timing, frequency, magnitude, direction);
- Operational efficiency;
- Frequency of incidents; and
- Patterns in system component performance.

Categories can be applied to scenarios, including security and perimeter protection, public safety, environmental conditions (e.g. rainfall and flooding), traffic monitoring and asset protection.

When making decisions on the categorization of content, jurisdictions should be aware of the following common assumptions:

- Categorization of content may be influenced by legislative and court decisions. Those influences may require limits or restrict categories of content or the ways in which those categories can be created and maintained.
- Categorization of content will likely involve significant internal and external inputs on issues of privacy and security, which may change over time.
- Demand for video content will likely be high from multiple sources inside and outside government, which may influence categorization decisions based on resources to meet requirements.
- Categorization of content for video is a relatively new phenomenon for most jurisdictions and will increase in complexity as the video system grows.

Special Consideration for Usage — Interrelationship with External Databases:
The digitization of data raises the possibility of linking visual imagery with a range of unrelated informational databases. Two immediate examples of this phenomenon will be described, as they point to the need to address this issue in design and operation of those systems.

The first example is license plate recognition (LPR) technology. Enhancement in imaging capability and digital processing make possible real-time monitoring of license plates and comparing them to other records databases like stolen vehicles, registration data, and warrant or other watch lists. Therefore, LPR gives a jurisdiction the ability to conduct a range of enforcement activities. While those activities are certainly related to legitimate government enforcement and revenue collection, they may not be related to the specific government purposes for which the camera system was created. How those data are captured, categorized, stored and used raises a host of privacy concerns for citizens and advocacy groups. Understanding the databases utilized for comparison and the reasons for doing so is important. That usage must relate to the governmental purpose of the system. It must also be consistent with guidelines for privacy protection.

Where jurisdictions have expanded the use of camera systems to enhance enforcement of traffic (e.g., red light and speed enforcement cameras), there has been significant backlash. Similarly, LPR use to cite drivers for other administrative offenses is controversial, such as failure to complete emissions testing. Moreover, the relation of visual data to these other databases may serve to undermine public confidence and support for the overall system.

A second example of concern over relating visual data to other databases comes from the advancing technology of facial recognition. Consider the use of facial recognition technology to investigate criminal activity captured by a video system. What databases can be used to establish the identity of an offender? Can images be compared to mug shots? Should law

enforcement be permitted to utilize driver's license photos? What about accessing publicly available photo collections on the Internet? Technologically, all these searches are currently possible. What searches should be permitted and under what circumstance? Relating camera data to these other systems raises significant public policy issues concerning privacy and civil liberties.

The two examples above demonstrate the range of concerns over using video system data with other databases. Before an agency determines whether to do so, the following issues need to be addressed:

- Does this database relationship serve a legitimately defined governmental purpose?
- What impact does relating video data to any given database have on privacy and civil liberty concerns?
- What impact does relating video data with any given database have on public support?
- What safeguards are in place to ensure appropriate use of related databases consistent with government purpose and privacy guidelines?

As systems mature and as the capability to relate to new databases expands, the issue of database relationships will likely grow. As systems change over time, there is a need for ongoing attention to these concerns. The International Association of Chiefs of Police (IACP) has published the IACP Technology Policy Framework, which suggests a series of principles governing the implementation of any technology with potential impacts on privacy [22]. Such guidance may provide a useful tool when developing policies for video systems.

3. Sources Considerations

Background and Description:

The term "sources" as it pertains to public safety CCTV video refers to sources of video streams or feeds, sometimes called digital media content (DMC), coming into a given system. Depending on the objectives of that video system or federated system, the types of sources of video will differ. As recognition of the value of video grows, so too does the understanding that sharing of video sources, where feasible, enhances coverage, reduces cost and provides for better public safety.

While the sources for most public safety systems are cameras owned and operated by government or quasi-governmental agencies, a growing number of jurisdictions are including private or commercial sources as well. Recent events, such as the 2013 Boston Marathon Bombing, demonstrate the value and importance of images taken by non-government sources. For private sources, the focus is usually on the views or cameras that cover public areas, such as streets, sidewalks and plaza areas open to the public. Those sources are being brought into

governmental systems in variety of ways: wired access, wireless access and virtual private network (VPN) connection though the Internet.

When determining what sources to consider including in a system, it is important to have a clear understanding of the system's governmental purpose, which in turn drives which stakeholder entities to involve and which sources are needed. Once the purpose is clearly understood, the entity undertaking the design and implementation ("the implementer") of such a system should conduct an assessment to determine what video within those parameters may already be available, and to determine if video sharing will be a strategy used to provide sources, as opposed to installing new cameras. Of course, only willing participants can have their sources assessed or ultimately accessed.

Access to sources and the existence of a common mission for all stakeholder groups is a key determining factor as to whether the implementer will build a separate system or seek to find ways to share existing video sources to support a joint operations mission. There is a balance to be determined among the numbers of sources, the complexities related to managing relationships for use of and sharing of video sources, the cost efficiencies related to video sharing, and the long-term system support and funding. It is often simpler to build your own system in some cases, but other efficiencies and an enhanced ability to collaborate may result when considering partnerships with other regional stakeholders to share video sources. It is important to be certain that these factors have been taken into consideration.

When implementing a video system, there are many products and options in today's marketplace. Anyone embarking on developing a system will find they can spend a considerable amount of time evaluating vendor claims and offerings. It is important to determine the mission, the functional requirements to meet that mission, and the budgetary and time constraints to meet the mission. At some point, you will need to select the best product (at the best price) to meet the needs of the mission and budget, and lock that down for a pre-determined period of time. Doing so allows for focusing on the development of the system itself and having the proper support mechanisms in place to ensure successful use of the video sources for the desired mission. Having a roadmap that determines how a given effort will track video source quality vs. mission, and having processes and funding in place to keep up with that mission will be key. Many projects have spent a great deal of money building a system with no means to keep it updated over the long term. By the same token, it is recommended that an effort start small, focus on a proof-of-concept for a given mission and geography with sources that make the most sense as a foundation (e.g., city center, around critical infrastructure, etc.), and make that effort successful. Users will play a key role in providing input as to where additional video sources are needed as the video system expands.

Assumptions:

When determining what sources of video are needed and how they will be obtained, the following assumptions need to be considered:

- The identified governmental purpose is the driver for system use and the identification of uses consistent with that purpose (i.e., incident management and response, covert, event-based, temporary vs. permanent, critical infrastructure protection, mobility and traffic management) will drive the identification of sources with similar missions and inclusive geographies.
- An individual or agency, which is a clear owner and sponsor, is identified for the development of a public safety video system. That sponsor will drive important decisions regarding mission and scope, which will affect the video type and location of sources that will be needed.
- For a given system, well-defined geographical boundaries, goals and priorities are clearly stated at the beginning of the system's design.
- Video sources, for the sake of this document, provide data pertaining to public safety video (as opposed to site security video, broadcast video, etc.). That is, this is video that is used in a public safety-centric mission. The types of sources to be included in a particular situation will be determined by the project sponsors or system owners based on their mission.
- Funding considerations will drive priorities and strategies for types of sources and priorities. Understanding these considerations upfront is key.
- In many cases, partnering with other regional stakeholders is a cost-effective approach to quickly increasing coverage in a particular geography because there is similar interest in observing areas among different users. Before investing in implementing a large number of video sources, it is important to assess where those potential partnerships may exist and whether they might be a viable option.

Strategic Objectives:

Strategic considerations begin with the issue of identifying and accepting a governmental purpose for the overall operation of the system. Consistent with this purpose, the governmental entity should assess the jurisdiction for existing and planned camera systems that could be leveraged in support of the governmental objectives. Once other sources are identified, the government entity must work to establish partnerships with those other systems and individuals.

Establishing a partnership requires an understanding of the objectives of all partners to see where their interests and source use can be identified. Once this assessment is completed, the partnership arrangements can be defined and formalized. Partnerships should then be

memorialized through MOUs or Intergovernmental Agreements (IGAs). These documents should outline the major points of agreement by and among all system partners.

The documentation of a common governance structure for system development and operations is of critical importance. That structure should be empowered to address technical and operational issues as they arise in the development and operation of the systems. Issues addressed in the MOUs, IGAs or governance structure should include:

- Issues of ownership and use with respect to equipment, software, images and data;
- Issues of control and responsibility for maintenance and repair;
- Temporal issues—permanent or continued use, as opposed to event-based or invited use;
- Types of systems covered — permanent, temporary or mobile cameras; and
- Funding and cost sharing for ongoing maintenance and system enhancements.

With respect to these issues, the governance structure needs to address roles and responsibilities for participants. In addition, these agreements should carefully outline communication channels so that operational issues such as outages can be addressed across the system.

The agreements should also address the issue of cost with respect both to development and operation. While there are many different models that can be followed with regard to all aspects of governance, a common thread is clarity on issues. Creating clearly defined expectations is important to smooth cooperation among multiple partners.

Because so much of the structure derives from clear articulation of guidance and clear agreement among partners, executive level participation is crucial. It is often only at the executive level where definitive commitment by an agency can be made. Accordingly, participation of those individuals in the process expedites decision-making and provides greater force to any agreements.

Operational Measures:

As entities seek to implement MOUs and IGAs, they need to have clear policies to implement those agreements. Those policies should address:

- Issues of ownership and use with respect to equipment, software, images and data.
- Issues of control and responsibility for maintenance and repair.
- Temporal issues — permanent or continued use, as opposed to event-based or invited use.
- Types of systems covered — permanent, temporary or mobile cameras.

- Ongoing verification/maintenance of video from sources.
- Planned outage notification to all user communities.
- Process for users to provide feedback on source quality/outages.
- MOU/IGA entry/exit requirements.
- Identification of relationship managers and troubleshooting processes between partners for system issues.
- Guidelines for who is responsible for maintaining video quality and service-level agreements (SLAs) for addressing camera outages.
- CONOPS for use of sources and priorities/permissions for sources.
- Ownership designation for sources (e.g., police divisions own the decisions related to sources within their geographies with regard to priorities, sighting and recording).
- Funding streams identified to address recurring costs. Including multi-year funding plans for essential service items like cellular technology that may not be funded from one year to the next.
- Clear rules for source to be recorded and/or disseminated.
- Funding and storage considerations.
- Supportability for added sources.
- Public space vs. commercial or private space considerations.
- Rules of engagement for sharing with partners, such as assessing cost/benefit on sharing feeds with partners.

Technical Measures:

In accepting sources, the following issues need to be considered:

- Technical standards regarding equipment, infrastructure and data for inclusion into the system.
- Ownership of various technical infrastructures for sources, as well as infrastructure supporting proper functionality of sources.
- Bandwidth and backhaul capabilities will play a key role in determining types of sources that can be accommodated (e.g., high-definition video over wireless).
- Standards for frame rates, camera types and products to support functional requirements and achieve support efficiencies.
- Performance monitoring, which would ideally be automated.
- Technical support to enforce expectations for ownership and use for partner video systems and the images they generate.
- Network security measures to support sensitivity and criticality of video system/sources and to protect privacy interests (Are the sources mission critical? What is an acceptable response time to address source outages?).
- Application of source masking and redaction to protect interests of partners in source confidentiality.
- Process and permissions to ensure safeguards for protected partner information that may not be applicable to all participants or which may exist in a geography or source type (e.g., HIPAA).

- Technology solution to address mobile applications.
- Interoperability across source feeds.

Stakeholders:

Sourcing requires input and collaboration among a wide array of stakeholders. Each has an interest in the program outcomes and oversight. Agencies developing video programs should engage the following groups:

Internal

- Executive sponsorship (to set direction, but also assist in negotiating with source owners or owners of facilities used for source locations);
- Departmental management (functional and technical);
- Operational users (first responders, criminal/civil investigators, transportation, public works, etc.); and
- Technical implementers (information technology, procurement, project managers, facilities management, transportation engineers, permitting and planning).

External

- Regional public safety agencies (e.g., traffic management; 911 call centers; local, county and state governmental agencies; flood/water districts; critical infrastructure agencies and districts);
- Commercial entities with public safety concerns (e.g., ports, universities, airports, medical centers, stadiums, convention centers);
- Community partners (e.g., management districts, Chambers of Commerce, business improvement districts, neighborhood associations, etc.);
- Media (identifying issues, providing public awareness, ensuring appropriate oversight); and
- General public (balancing program goals with privacy issues).

Impacts:

Impact considerations start with one simple thought: "quality in – quality out." Proper planning must address what video sources are needed based on the mission and what the users' functional requirements will be, or even the best video system may fall short. Additionally, continually chasing new technologies could create a distraction from developing a solid design with quality video sources delivered to the right place at the right time. It is important to get trusted advisors to provide the correct information to make informed and unbiased sourcing decisions. Also, taking time to build lasting partnerships with long-term regional stakeholder partners could further solidify the ability to deliver quality video sources in a public safety video system. A viable partnership allowing agencies to view each other's cameras provides real value to a video program and reduces coverage costs.

4. Notice Considerations

Background and Description:

This section is intended to discuss the notification to the public and other stakeholders related to video capture. The issue of notice has to do with the appropriate notification regarding the purpose, installation and operation of a given video system. Sponsors/owners of these systems may or may not wish to engage in public notification. Such notification may or may not be a legal requirement. Consideration should be given as to whether to engage in a large notice campaign that may draw undo attention to an otherwise fairly innocuous system as far as the public is concerned. In other situations, an aggressive public notice campaign may add significant and important public support. Making such a strategic decision involves understanding the culture of the community and determining whether or not public notice is helpful or harmful to furthering the success of the system. In some cases, it is better to have individual notice strategies for key stakeholders who may have sensitivity to a system in the proximity of their operation (e.g., a church or synagogue).

The first consideration in the evaluation of a notice strategy would be a determination of legal notice requirements. Does a statute, ordinance or regulation require notice generally and/or specifically when a camera is being placed or operated? Because such externally imposed regulations may change over time, this determination, particularly with respect to system operation, must be flexible enough to react to potential changes in notice requirements. Legal requirements may also specify the form of notice. For example, there may be a requirement for a governmental entity to publish notice in a newspaper of record in the jurisdiction announcing the intent to place cameras. Notice requirements might also be accomplished through the posting of nearby signage.

Notice may also be required by a jurisdiction's operational strategy. In cases where a purpose of the system is deterrence, public notification may be part of an overarching strategy. That notice may include specific signage at the location or a general public dissemination of the information. The presence of cameras can also be messaged to the public. In cases where there is a perception that signage is important to address public concerns over privacy, there may be a determination by a community that signage should be posted to advise the public of the presence of cameras recording activity. Signage is not the only means of messaging the presence of the cameras to the public. The use of distinctive designs and in some cases even flashing lights can be used to announce the presence of cameras.

Where signage is used to provide notice, the jurisdiction needs to be mindful of the language used. Language should be targeted at addressing key sensitivities and avoiding overstating or misrepresenting the intent of the system and its impact on the public. If feeling safe in a downtown area at night is an important issue, then the language should be selected with the

aim of providing a feeling of safety. If deterrence in known hot spots is an issue, then more forceful language can be used to indicate a targeted focus on an area or issue that suggests a specific course of action. While the language of the notice may be adapted to the purpose of the system, those notices must not create false expectations on the part of the public. If video is not being recorded or monitored, the notice should not represent otherwise. False or improper notice may have significant legal repercussions. For example, there may be legal consequences with representing the existence of surveillance where none actually exists. The deployment of "dummy" cameras or other methods of creating the false impression of surveillance is one such example.

Notice also relates to a communications plan to provide notifications to partner agencies and their users regarding system issues, changes in permissions in the system, the addition of more sources and planning activities for key events. Even changes to a notice policy previously established between partners may be a consideration. Given that stakeholder agencies/partners have developed concepts of operation based upon their understanding of system operation and policy, having an adequate notice policy is key. This is essentially a communications plan, such as would be developed for any process or system.

Assumptions:

When determining what a notice policy should include, the following assumptions should be considered:

- The executive sponsors should develop their notice policy based on their understanding of cultural sensitivities related to the type of system being implemented, as well as existing legal requirements.
- Notice may result from an inquiry by the media as a consequence of seeing that a particular procurement related to the system had been announced in a public notice (e.g., council agenda). This is a reactive notice that should be crafted using the same logic previously discussed pertaining to sensitivities and opportunities.
- The requirements of notice can be derived from operational imperatives, such as enhancing deterrence or enhancing system privacy protections.

Strategic Objectives:

As a matter of policy, the issue of notice should be addressed and resolved instead of being a matter of default. In addressing the issue of notice, there needs to be a survey of legal requirements, an assessment of community sensibilities and a review of operational imperatives. Consideration should be given to issues of system transparency, deterrence effect, privacy protection and cost (particularly when a community determines to post signage).

With respect to a notice plan, the following should be considered and documented:

- Whether to notify the public, reasons to notify or not notify the public, how to notify the public, when to notify the public, etc.
- Whether the notification of the location is appropriate (as this could compromise the security of a system). There may be many cameras in the public space where it may not be obvious which of them are part of a particular system. Additionally, the infrastructure behind the cameras, if the locations are included in the notice, should likely not be shared.
- Given the potential for unexpected results related to notice, the process should be used judiciously to avoid unnecessarily creating alarm.
- With regard to video partnership MOUs, some of these may mention a need to review notifications annually. This activity needs to be owned by the operator(s) of the system.

Operational Measures:

When an agency decides to provide notification, public and private partners should develop a communication plan to address the following issues:

- Legally required notice;
- Notice required by operational or other concerns;
- Intended result to be accomplished by the notice;
- Determination of the best message and media for notice;
- Timing of the required notice (before deployment, during operation); and
- Cost of notice (e.g., the cost of producing, placing, and maintaining signage).

With respect to notice of system design and development, there needs to be consideration given to a balance between transparency and system security. Information about the technical design should be revealed in a public notice only as legally required and operationally essential – less is generally best for security considerations.

A process should be put in place to determine message, timing, approvals and notice dissemination method. Considerations should include:

- Who should be notified (e.g., public, internal, and/or partners) and how should they be notified (e.g., signs, Internet and/or publication); and
- What will be the communications medium and who will coordinate the notice.

A process should be developed to handle notifications to or from partners on operational changes to the system. This may include notice to the user community and partner community about the availability, accessibility and impact on other systems (operational).

Technical Measures:

- Design of the device, which could impact what notification can be provided;
- Sustainability and maintenance issues;

- Potential impact to systems owned by external entities and partners when a notice of a system outage is sent;
- Notification of system health (outages, camera additions, cameras offline, etc.) to internal and external partners; and
- Situational (technical notifications to users).

Stakeholders:

Notice requires input and collaboration among a wide array of stakeholders. Each has an interest in the program outcomes and oversight. Agencies developing video programs should engage the following groups:

Internal

- Executive sponsorship (to set direction, but also assist in negotiating with location owners or owners of facilities used for source locations; manage any media or public concerns about the initiative);
- Departmental management (functional and technical);
- Operational users (first responders, criminal/civil investigators, transportation, public works, etc.); and
- Technical implementers (information technology, procurement, project managers, facilities management, transportation engineers, permitting and planning).

External

- Property owners;
- Utilities and public works (for support infrastructure);
- Regional public safety agencies (e.g., traffic management; 911 call centers; local, county and state governmental agencies; flood/water districts; critical infrastructure agencies and districts);
- Commercial entities with public safety concerns (ports, universities, airports, medical centers, stadiums, convention centers);
- Community partners (e.g., management districts, Chambers of Commerce, business improvement districts, neighborhood associations, etc.);
- Media (managing public perception and concerns when necessary; proactively informing the public of the intent of the system); and
- General public (balancing program goals with privacy issues; managing expectations).

Impacts:

Where notice is legally required, compliance is essential. Perspectives on the operational impacts of notice vary significantly. Some believe that that public notice significantly contributes to system transparency and deterrence. Others contend that empirical evidence on these issues is inconclusive. Where a decision is made to provide notice by way of signage,

caution needs to be exercised to ensure that false expectations are not created. If camera images are not recorded or monitored, signage should not suggest that they are. Improper notice might result in civil liability.

5. Monitoring, Analysis and Analytic Applications

Background and Description:

Programs for monitoring, analysis and analytic applications vary greatly based on system objectives and established governmental purpose. Some video systems have developed around the concept of active, or even proactive, monitoring. For those systems, real-time monitoring is a significant priority. Other systems are focused more on forensic use and their priority is on analytic tools to retrieve captured images. In order to balance these use cases, many systems apply a blend of active and forensic approaches based on evolving operational needs.

Common to all systems is the challenge of maintaining programs for monitoring, analysis and analytic applications in the face of growing and expanding video platforms. As the number of cameras expands in a system, so too does the challenge associated with monitoring and analysis. Human factors research on the subject of camera viewing and analysis suggests that the ability of humans to view and analyze images has limits. Therefore, the expansion of camera systems requires either a commitment of a significant number of personnel resources (resources that may not be available to most systems), or reliance on analytic tools to assist in both the real-time and forensic analysis of visual imagery.

Tools to assist in the monitoring of camera systems come in a variety of forms. Video Management Systems (VMS) allow for the organized inventory and display of camera inputs across an entire enterprise. VMS can utilize Geographical Information System (GIS) mapping programs so that camera locations can be identified and camera views quickly assessed. VMS allows an operator to identify multiple views in an area of interest and access multiple camera views simultaneously. VMS are often connected to other systems that provide alerts and alarms, such as automated access control systems (ACS), fire alarms, motion detection systems, intrusion detection systems and panic alarms. Monitoring activity is also now being related to Computer Aided Dispatch (CAD) systems, social media monitoring systems and audio detection systems (e.g., gunshot detection). Some alert and alarm functions are automated through the VMS to facilitate monitoring. In other instances, the interface requires manual manipulation of the VMS.

In addition to relating monitoring to external alert and alarm systems, there is a growing suite of video analytic tools being designed to assist in accomplishing the task of monitoring and analysis. These tools allow for detection of anomalies or preprogrammed conditions, and

provide for alerts and alarms to monitoring personnel. These analytic platforms essentially fall into two categories: rules-based platforms and platforms based on machine learning.

The rules-based video analytic platforms involve programming camera sensors with algorithms to detect phenomena like the crossing of trip wires (or "geo fences"), loitering, traffic or movement in counter-flow (opposite direction). These programs are the more mature of the two video analytic categories. Rules-based analytics offers the prospect of being able to establish conditions (rules) such that, if violated, will produce an alert or alarm to a camera operator. The challenge of these types of programs is that they often take significant resources to develop and implement. Moreover, they can be affected by changing environmental factors, such as lighting, vegetation, etc. Additionally, the movement of a camera that changes its field of view may distort that analytic. Some users have found that high false positive rates make the system operationally ineffective (i.e., alarm fatigue).

The application of machine learning to video analytics is a relatively new concept. It involves the analytic program essentially learning what is normal in a video scene, and then alerting or alarming when an anomaly is detected. That anomaly may be an object or a movement that is outside the learned normal parameters. This machine learning approach can serve to reduce costs due to the more detailed implementation requirements of rules-based analytics. It also is designed to better adapt to environmental change as it learns the environment. As the utilization of this technology increases over time, better assessment can be made of the efficacy of this new technology.

Monitoring both in real-time and forensically may be enhanced by the application of object recognition and facial recognition programs. These technologies afford the possibility of identifying faces in the crowd or finding persons by searching for identifying clothing (e.g., a red coat or blue baseball cap). While this technology is still developing and may not currently have sufficient reliability for a function like real-time mass screening of individuals, it may prove beneficial in helping operators narrow their focus of attention to monitoring a subset of individuals or objects that are significantly similar to the operator's inquiry.

One final set of analytics bears mention, particularly with respect to forensic analysis. Utilizing image metadata, there is a growing suite of tools that can expedite the process of video monitoring and search. These tools allow focus on select portions of larger visual data fields to track things like movement. There are also tools that allow for the video to be synopsized so that hours of video can be presented in a matter of minutes by applying algorithms to shapes and movement within a fixed view.

Through the application of some or all of the technology tools identified above and in conjunction with the application of personnel resources, organizations can optimize their monitoring and analysis programs. The blend of resources should be adjusted based on system purpose and objectives. It may also be necessary to adjust the scope of project development based on the ability of an organization to develop its monitoring and analysis capabilities. Otherwise, the monitoring and analytic capabilities needed to analyze and understand all the data a system captures may not be met.

Assumptions:

The following are assumptions regarding issues of monitoring and analysis:

- Some degree of monitoring and analysis is essential to operate any video system.
- Almost no system has the resources to ensure that all cameras are monitored by human operators 24x7x365.
- Technology solutions can provide satisfactory enhancement for monitoring of critical conduct or objects.
- The balance of the focus on real-time use or forensic use will vary depending on the purpose of the system, but many systems will seek a blend of both.
- The focus of the system (real-time or forensic) will affect the balance of capabilities selected for monitoring and analysis.
- The balance of capabilities selected by an organization will be affected by the availability of resources.

Strategic Objectives:

The purpose of the video system will be a critical driver for decisions on monitoring and analysis. The greater the focus on proactive use of information from the camera system, the greater the need for human and technology support for monitoring and assessment. In developing the system, attention needs to be paid to ensuring that monitoring and assessment support is aligned to purpose. The absence of appropriate monitoring and assessment capability will significantly affect system efficiency and effectiveness. Because those requirements are directly impacted by system size and system expansion, they need to be considered as part of system planning.

The plan for monitoring and assessment needs to be transparent and communicated to the public. Individuals need to understand they cannot expect constant uninterrupted monitoring of every camera. Assessment and analytic processes need to be aligned with governmental purpose and consistent with privacy concerns and protections.

Operational Measures:

Operational measures include:

- Creating policy consistent with system purpose to ensure proper monitoring.
- Where the system utilizes automated systems or analytics, policy and CONOPS should be created to address when human review of alerts or alarms is required.
- If using automated systems or analytics, CONOPS should include a verification process.
- Policy should address who performs the assessment and what type of assessment and analysis is authorized (operators should be both authorized and qualified).
- Measures should be taken to communicate to the public the program for monitoring and assessment.
- Processes should be in place to audit and monitor system compliance.
- Processes in place including disciplinary action to ensure compliance with policy.

Technical Measures:

The following technical measures should be considered:

- Development of interfaces to other alerting or alarm systems as is consistent with the operational need and governmental purpose.
- Development and application of analytic programs consistent with operational need and governmental purpose.
- Development of capacity to collect and relate metadata to captured images, and also to integrate alert and alarming systems and analytics.
- Collection and use of metadata with development of interfaces to other alerting or alarm systems as is consistent with operational need and governmental purpose.
- Development of automated oversight and audit systems to ensure monitoring and data use is consistent with established policy.

Stakeholders:

Stakeholders include individuals within the jurisdiction's governmental structure, as well as numerous external constituents who may have interest in data monitoring and analysis of video data. Stakeholder groups include:

<u>Internal</u>

- Policymakers;
- Operational users (first responders, criminal/civil investigators, transportation, public works); and
- Technical implementers (information technology, procurement).

<u>External</u>

- Operational users (first responders, criminal/civil investigators, transportation, public works);

- Legal counsel (to review policy to ensure compliance with legal requirements on monitoring);
- General public (concerned about data use and privacy); and
- Advocacy groups (EPIC, ACLU, etc. – concerned about data use and privacy).

Impacts:
Decisions on monitoring and analytics have impacts on the ability of the system to support a range of operational requirements. They can also affect public perceptions of the efficacy of the video system. Robust monitoring and analytics will allow for significant enhancement in the real-time ability of operators to achieve situational awareness. However, the development and implementation of such is not without cost.

Resources for monitoring and assessment may affect the size of a given system. The larger the system, the greater the need for monitoring and assessment; thus, the attendant cost will increase. Where resources are constrained, the size of the system needs to be balanced with resources for monitoring and analysis. Thus, the availability of resources for monitoring and analysis should be considered in the early stages of system planning and architecture.

In addition to the cost issues, decisions on monitoring and assessment also require a balance between the desire to maximize, or at least optimize, situational awareness on one hand and concern over privacy and civil liberties on the other. At times these concerns can be at cross-purposes. Understanding community sentiment is important in gauging the appropriate balance. It may be that, even if resources are available for enhanced monitoring and assessment, there is inadequate public support.

Even in a robustly monitored video system, it is important that public expectations of their safety be appropriately managed. The creation of situational awareness does not necessarily translate into enhanced response. While it is a precursor for enhanced response, it must be successfully integrated into an operational CONOPS and requires adequate response assets. "Knowing about something" does not automatically equate to an enhancement in "doing something."

6. Retention of Video Data (Imagery and Metadata)

Background and Description:
The development of advanced video systems creates concerns about real-time use, as well as concerns about the issue of what to do with the stored data generated by this system. While a video system does not necessarily need to store data (e.g., the video system could be designed for real-time viewing only), the norm is increasingly to capture and store data for some period

of time. This period for retention of stored data can vary widely and is influenced by a range of variables, including technological constraints, operational requirements and legal imperatives.

In the pre-digital era, major restrictions were placed on data retention by technical limitations. For example, in the days of analog video, the physical ability to store VCR tape and the limited ability to catalogue and retrieve data made long-term storage impractical. Indeed, tape storage was often limited to hours, days or weeks depending on the resources of the video operator and the perceived need for data. However, recent changes in storage technology and computational capacity have changed those limitations. With developments in both computer storage capacity and compression technology, larger amounts of data can now be stored at less cost (however, it should also be noted that compression could be damaging to DME, so great caution must be exercised with respect to application of compression technology). As cloud storage proliferates and camera manufacturers enhance the ability to capture imagery using smaller processing and storage space, this data storage capability looks to be increasing dramatically for the near future. In addition to the visual imagery this data can generate, there are also fields of metadata to be stored and analyzed.

As the technical constraints on data storage have been reduced, the operational and legal issues around storage of data have increased in significance. This situation is not unique to video. Digitization and computational capacity have revolutionized storage of materials formerly maintained as paper documents and analog voice recordings. Not only can more records be easily stored, indexed and retrieved, but the versions, drafts, changes and inputs can also be easily stored. In most all jurisdictions, records retention statutes, ordinances or regulations cover recordings conducted by or relating to the operation of government.

In a number of jurisdictions, video data are considered essential government records. In those jurisdictions, the retention schedule must meet legal requirements. These legally imposed retention requirements may apply to all video data, or only certain types of data (e.g., license plate recognition data). In some jurisdictions, the agency collecting the data may be allowed to have some degree of input in establishing or modifying a retention schedule.

While many jurisdictions may have legal requirements for the length of record storage, those requirements frequently do not include a requirement with respect to the quality of images stored. This is likely due to the fact that those legal requirements were originally designed to address paper records and thus do not translate perfectly to digital video data. Accordingly, as some jurisdictions attempt to increase capacity or reduce cost, the storage of video data is being accomplished at a reduced frame rate. This decision has operational implications for the utility of the data stored.

In jurisdictions where there is no legally imposed retention requirement, or where the requirements provide an agency some level of discretion in the establishment of retention periods, operational considerations should be addressed in the establishment of retention requirements. This could mean that cameras installed for different operational purposes might have different retention schedules. For example, video of the perimeter of a critical infrastructure facility (e.g., for the purpose of determining movement patterns and conducting counter-surveillance operations) might have a longer retention period than camera data from a transit turnstile that looks for turnstile jumpers. The intended or anticipated operational uses of video data should be factored into the retention schedule. Operational requirements have implications not only for the length of time which data is stored, but also for the quality of these data.

Finally, retention schedule policies should consider legal issues over the availability of data for civil and criminal proceedings, and the penalties for failure to comply with statutorily imposed retention requirements or juristically established data retention schedules. Failure to establish or follow a retention schedule may expose a jurisdiction to civil and in some cases criminal penalties. In a criminal context, the failure to properly maintain data in accordance with proper retention requirements may result in dismissal of a prosecution. In addition, it is critical to maintain video evidence in a manner that does not impact the integrity of the evidence. Applying compression during transfer from the original acquisition to another storage location, for instance, can result in the permanent loss of important data and ultimately diminish the probative value of the evidence. In the civil context where there is a growing incidence of electronic discovery ("e-discovery"), there are increasing requirements to maintain data and increasing scrutiny on the absence of data, particularly where there is no retention schedule or where an established retention schedule has not been followed. Thus, the failure to properly retain data may subject the jurisdiction to civil penalties.

The specter of criminal sanction and civil liability should compel both the establishment and compliance with a retention schedule. It should also cause agencies to review the quality standards they establish for retained data. If the data may potentially need to be preserved beyond the normal schedule for certain purposes (such as investigations, criminal or civil legal proceedings), retention schedule policies must include procedures for the review, selection and preservation of data beyond the original retention period.

Assumptions:

The following are important assumptions for retention planning:

- A jurisdiction will usually want to record some or all of the data collected by a video network.
- A jurisdiction will confront some resource limitations that will constrain their ability to store and manage retained data.
- A jurisdiction will have operational and legal requirements that will impact length of storage and quality of data.
- A jurisdiction may not have complete control over the requirements for retention length and those requirements my change over time.
- Technology will continue to advance, enhancing the capability of a jurisdiction to retain larger amounts of data at higher quality.

Strategic Objectives:

Any entity that stores video data should have a comprehensive written policy governing the terms and condition for data retention, and the method for removing data once the retention period limit is reached. The policy must comply with legal imperatives and, where possible, be aligned with the operational requirements that necessitated the storage of data. The policy should outline the legal, operational and technical basis for retention. It should also outline the terms under which data can be stored beyond the specified retention period (e.g., evidence in legal proceedings and investigations).

Operational Measures:

Any comprehensive written policy for retention should have the following features:

- Policy on evidentiary use should be consistent with jurisdictional requirements.
    - Policy in place for how to handle the retention and destruction of recorded video that has not been deemed evidence, but whose retention period is about to expire.
    - Policy in place for how to handle the secure retention and conservation of recorded video that has been deemed evidence.
    - The expiration date on video data retention may need to be extended if it is potential evidence. One possibility is to create an “investigative” category to extend the retention period for cases where there is an active investigation and the video has the potential to become evidence (i.e., need a policy for video data with an expiring retention limit when it may potentially become evidence, but is not yet evidence). This “investigative” category should not be classified as public record, but the evidence category may be public record. For example, the video record may be utilized as “investigative notes” instead of evidence. If under “investigative notes,” then it is not publicly accessible unless subpoenaed (note: this would vary by jurisdiction depending on laws and court decisions).

- Policy should state what defines video as public record and when it becomes public record. There are potential data spillage issues also. All images and associated data are property of the owning agency. Under what circumstances are others allowed to access these data?
- Rules of disclosure need to be in the policy. For example, if video retention is 28 days, then it is up to the video owner to decide what they want to keep longer than the 28 days.

Technical Measures:

Technical policy considerations include:

- Storage infrastructure (data integrity for embedded, network detached storage, storage area network and software defined network);
- Third party storage device has to be interoperable with other devices, including legacy and future systems;
- Forward and backwards compatible;
- Extensibility;
- Maintain adequate future storage capacity relative to the mission;
- Redundancy for recorded video (e.g., fail-over especially for mission critical data);
- Service level agreements and quality of service (QoS) need to be well-defined in the policy;
- Maintain appropriate records management; and
- Maintain an audit process.

Stakeholders:

Stakeholders include individuals within a jurisdiction's governmental structure, as well as numerous external constituencies who may want to access video data. Stakeholder groups include:

<u>Internal</u>

- Policymakers;
- Operational users (first responders, criminal/civil investigators, transportation, public works); and
- Technical implementers (information technology, procurement).

<u>External</u>

- Policymakers/Records supervising agencies (e.g., state legislatures, state/local archivists);
- Operational users (e.g., first responders, criminal/civil investigators, transportation, public works);

- Legal community (e.g., judges, prosecutors, public defenders, and private criminal and civil attorneys—court orders, subpoenas, civil/criminal discovery & e-discovery);
- Media (Sunshine /Freedom of Information Act (FOIA) requests); and
- General public (Sunshine / FOIA requests).

Impacts:

Retention schedules have both operational and technical implications. For example, in cases where a retention schedule is extremely lengthy, the agency may be faced with decisions over increased storage costs to maintain the system, or choices about reducing camera counts in system operation or image quality in storage. The latter choices may have substantial implications for the collection of data or the use of data collected. The unavailability of data can have significant operational impacts.

Retention requirements may have significant impacts on the technical specifications of the video system itself. At a minimum, those requirements will impact the size of required storage. They will also likely impact how a system is architected and implemented (e.g., on-site or cloud storage). The design of the system will, in turn, have implications for system operation and cost.

The failure to have a retention schedule or to follow that schedule may have legal implications both for criminal prosecutions and the incursion of civil fines and penalties for the jurisdiction.

7. Dissemination of Video Data (Imagery and Metadata)

Background and Description:

As noted above, the development of advanced video systems and enhanced storage capacity has resulted in governments having access to and retaining large amounts of video imagery and associated metadata. That imagery is often of value and interest to other government agencies, as well as to private organizations and individuals. Thus, the sharing of images and other video data has become an issue for many jurisdictions.

Like the sharing of any data collected by governments, there are often different categories and rules depending on the content requested and the entity or individual making the request (the "requestor"). Procedures for release of information held by the government are generally regulated by statutes or ordinances pertaining to the agency, or to a set of agency rules (which may have been created in whole or part in response to statutory or ordinance requirement).

Dissemination procedures can and often do differ, depending on the content of the information. For example, rules for dissemination of information considered to be criminal justice information or evidence in a criminal proceeding are much different from rules that are

applied to categories of other information, such as regarding a public procurement or other public act. Rules can also be different where the information involves matters that may be private or impinge on some business or trade secret.

Special rules may be applied when the requestor is the subject of the video. While this may be based on reduced concern over privacy (i.e., releasing a tape to the subject of the video presumably raises no privacy concern), it also may be based on the notion that individuals have a special concern in knowing what information government has collected on them. This concept is generally not present in most FOIA or Sunshine statutes. Those statutes generally provide rights to documents available to any requestor. They do not make exceptions based on the requestor's status or whether the individual is the subject of the record or data requested.

Dissemination rules may also differ depending on the source of information. For example, where a system is taking in images from cameras owned and operated by external public or private agencies, there may be additional limitations on the ability of an agency to disseminate by virtue of MOUs with those external entities. Of course, governments need to ensure that the provisions in those MOUs are consistent with statutory disclosure requirements.

In addition to having rules that differentiate based on the content or source of the information requested, rules often may vary based on the status of the requestor. Rules can vary depending on whether the requestor is a member of the agency or department, or is viewed as an external applicant. Those questions will be analyzed more fully in the section on Access and Use. This section on Dissemination will focus on external requestors.

External requestors can be grouped in several different ways, but the following categories appear to be commonly used:

- Governmental agencies within the jurisdiction — this might include sharing among coordinating departments of a city (i.e., police department utilizing cameras owned and operated by a transportation department).
- Governmental agencies outside the jurisdiction — this might include sharing among different governmental agencies from differing jurisdictions (e.g., a state or regional transit agency sharing cameras and images with a city government).
- Law enforcement agencies—oftentimes there are special statutory and regulatory arrangements that allow for information sharing between law enforcement agencies for law enforcement purposes.
- Private individuals and entities whose activities or property is the subject of images.
- Private individuals and entities whose activities or property is not the subject of images.

The rules for information sharing among these categories of requestors frequently vary across a wide range of categories of information collected and maintained by public agencies. Those arrangements are shaped by statutes and ordinances, including FOIA or Sunshine laws, privacy laws, MOUs, as well as other governmental agreements and arrangements.

Dissemination of video data can occur in real time and forensically. In large camera networks, it may be possible to have images accessed simultaneously by a number of different agencies (internal, external and law enforcement). While this phenomenon of simultaneous image sharing principally involves governmental requestors, it may also include private parties. In a growing number of jurisdictions, there are movements to place images of cameras (particularly ones operated for traffic functions) on the Internet accessible to the public.

Live video sharing can lead to issues if the governmental camera owner has no capability to restrict activities like downloading of images or to disable sharing functions in the event privacy or surety concerns necessitate such actions. Where sharing occurs in the government context, the rules for recording and retention of data are often addressed in MOUs governing sharing. Those agreements often either prohibit the recording of images or limit the ability of the governmental agency to subsequently disseminate the data.

Sharing, particularly among governmental agencies, raises issues of subsequent dissemination. While generally no limits are placed on the subsequent dissemination of images shared with a private party, the sharing of images among governmental entities is handled differently. Many MOUs governing sharing of images among public entities address the issue of subsequent dissemination of data and the need to return images to the owner when the governmental purpose for sharing expires.

Policies regarding the dissemination of data should address the administration of requests and redaction. Dissemination requirements can and often do impose burdens on jurisdictions to respond to a wide range of increased demands for data. Dissemination of data can result in governmental agencies balancing the requirements of transparency and open government on one end of the spectrum with the need to protect privacy or criminal justice processes on the other.

Almost universally, legal disclosure requirements contain some exceptions for privacy and criminal investigation, and possibly other situations. Understanding those requirements and responding to requests to determine what video data must be made available will require trained personnel resources. While technology can expedite search procedures, it will not eliminate personnel requirements. Depending on the scope of the system and data retained,

personnel requirements may be extensive. In some jurisdictions, the cost of search and production of data can be shifted to a requestor. In other jurisdictions, however, that cost may have to be borne by the agency. Moreover, the failure to properly produce responsive information may expose the department to civil liability or other legal and administrative sanctions.

In addition to requirements for finding and producing responsive data, there also will likely be requirements for redaction. While redaction issues can arise in any dissemination context, it is most likely to occur in response to FOIA or open records requests. Responding to these requests will require not only personnel, but also additional software and perhaps hardware to redact responsive data. The question of redaction may involve not only imagery, but also audio data and associated metadata. In some jurisdictions, the cost of redaction can be shifted to a requestor. In other jurisdictions, however, that cost may have to be borne by the agency. Moreover, the failure to properly redact video information may expose the department to civil liability or other legal or administrative sanctions.

Assumptions:

The following are important assumptions for dissemination planning:

- A jurisdiction will usually receive requests for data from a variety of sources, including government, law enforcement, courts, and a variety of private entities and individuals.
- A jurisdiction will usually receive requests for data for a variety of purposes, including criminal investigations, legal proceedings (criminal and civil), media inquiries and a variety of other private interests.
- A jurisdiction will confront resource limitations that will constrain their ability to manage dissemination of data.
- A jurisdiction will have operational and legal requirements that will impact dissemination of data.
- A jurisdiction may not have complete control over the requirements for dissemination including:
    - Time frames for production;
    - Subject matter of responsive materials;
    - Redaction requirements; and
    - Cost allocation for required personnel material and service.
- Externally imposed requirements may change over time without regard to the effect on the system.
- Technology will continue to advance, enhancing the capability of a jurisdiction to disseminate data.

Strategic Objectives:

An entity must have a have a comprehensive written policy governing the terms and conditions for data sharing. That policy must recognize the differing rights and interests of a variety of requestors across the expanse of a variety of types of data. In instances where images are shared, the issue of data ownership needs to be addressed. The process for making requests and the fulfillment of those requests must be clear. Measures need to be in place to ensure appropriate safeguards over redaction and unauthorized dissemination, and the method for removing data once the limit of the retention period is reached. The policy must comply with legal imperatives and, where possible, be aligned with the operational requirements that necessitate the dissemination of data. The policy should outline the legal, operational and technical implications of dissemination.

Operational Measures:

Any comprehensive written policy for dissemination should have the following features:

- Identification of categories of requests, requestors, and content and rules applicable to for fulfillment or denial of dissemination;
- A process for request fulfillment (including redaction and cost allocation) and tracing of all dissemination requests and responses;
- A process for adjudication of disputes with respect to fulfillment of requests for dissemination (or decisions on redaction);
- Rules for determination of image/data ownership and, where appropriate, rules for subsequent dissemination or use of shared images (including return of images/data);
- Procedures to mark produced materials so that the disseminated materials can be traced to the persons and equipment involved in dissemination;
- Procedures to document redaction decisions and any forensic processing, including logging and tracking functions;
- Dissemination rules aligned to retention requirements so that materials are maintained and available for dissemination based on agreements and legally imposed requirements;
- Establishment of controls over dissemination and redaction of materials limiting this authority to specified groups of personnel and activities;
- Provisions for supervision and audit of all dissemination and redaction personnel, equipment and functions;
- Provisions to discipline individuals who improperly disseminate or fail to disseminate materials; and
- Provisions for periodic review and modification of all policies based on internal operational requirements and external changes, such as changes in laws.

Technical Measures:

Technical policy considerations include:

- System permissions and other safeguards to preclude unauthorized dissemination of materials;
- Automated audit functions of request dissemination and redaction activities;
- Automated search and redaction functions;
- Watermarking or other identification features to allow for tracing of disseminated materials;
- System capacity to meet dissemination requests in a timely manner; and
- System security to insure the integrity of disseminated data.

Stakeholders:

Stakeholders include individuals within jurisdiction's governmental structure, as well as numerous external constituents who may want to access video data. Stakeholder groups include:

Internal

- Policymakers;
- Operational users (e.g., first responders, criminal/civil investigators, transportation, public works); and
- Technical implementers (e.g., information technology, procurement).

External

- Policymakers/Records supervising agencies (e.g., state legislatures, state/local archivists);
- Operational users (e.g., first responders, criminal/civil investigators, transportation, public works);
- Legal community (e.g., judges, prosecutors, public defenders, and private criminal and civil attorneys—court orders, subpoenas, civil/criminal discovery & e-discovery);
- Media (Sunshine /FOIA requests); and
- General public (Sunshine /FOIA requests).

Impacts:

Dissemination rules have both operational and technical implications. Requirements for dissemination may affect the retention period selected by jurisdictions, if such a selection is permitted by law. It also may affect what or how much a jurisdiction decides to record. Release of data may affect the conduct of investigations or the way in which the jurisdiction decides whether and how to provide public information. Dissemination rules may also affect how a system is configured or operated. For example, rules on image sharing may affect how an

agency documents activity in the case of images from another entity's cameras, where those images are not recorded on the system. Limits on data sharing may have significant operational impacts internally and on relationships with a range of external agencies (public and private).

Dissemination requirements may have impacts on the technical specifications of the video system itself. At a minimum, those requirements will impact the issues of video data storage, the search and retrieval of data, and the redaction of information. The design of the system will, in turn, have implications for system operation and cost.

The failure to have a process for dissemination or to follow that process may have legal implications for criminal prosecutions, as well as possible civil fines and penalties for the jurisdiction.

8. A Well Defined Governance Structure is Important for Video Program Success

Background and Description:

In the early stages of video program development, agencies should focus time and attention on establishing the governance structure for their video programs. Governance can often be a misunderstood and overlooked aspect of program management, but when structured properly, it helps to clarify expectations, improves accountability, leads to better organizational performance, and ultimately results in a higher likelihood of video program success.

Governance is the combination of structures and decision-making processes that provide strategic direction and oversight during both program development and delivery in an organized and defined manner (Figure 2). These mechanisms connect strategic direction with administrative implementation to ensure program outcomes are met. Without these mechanisms, guidance and expectations are often unclear, and accountability is lacking. Programs not grounded in effective governance often do not maximize efficiency and effectiveness, and can erode confidence in the agency.

Figure 2. Governance models

Careful consideration needs to be given to current organizational structure and the program's organizational framework. It is important to begin with defining the operational authority and the roles of the governing board, administrative staff and project partners.

In general, the governing entity will establish the need for video services, identify and articulate community goals and expectations, and provide broad program oversight. The need for video services often comes from community engagement. For example, this engagement could be business owners seeking surveillance to reduce crime and vandalism in their commercial districts. Video may also be used for greater police oversight, including calls to community action from high profile incidents, such as law enforcement overreach. Internal calls for video deployment may be voiced to collect video evidence or as active surveillance efforts. Regardless of the impetus for a video deployment, the governing entity will set overall program goals and establish general operating parameters, such as whether notice should be given on camera locations. The governing entity should refrain from trying to manage daily operations, but instead provide policy guidance with sufficient flexibility for program staff to be able to react to and accommodate daily issues.

Staff are often the subject matter experts and are called upon to provide policy advice to elected and higher ranking appointed officials. They help shape the debate by outlining the parameters for program development. These parameters may involve a range of issues, such as financial limitations, ease of deployment, maintenance, records retention, legal considerations, etc. After public policy is set, it becomes the responsibility of the staff to execute the policy

direction and manage daily issues that arise. Staff will develop procedures, reporting chains, delegate administrative duties, etc. Although staff members are subject matter experts, they need to respect the governing body's role in setting public policy. At times staff may not agree with the strategic direction, but staff has an obligation to implement the direction set by the governing body to the best of their ability.

There is often a blurring of lines between the political sphere and administrative functions. Where these spheres overlap, there may be friction, but this overlap is also where the governing entity learns about administrative concerns, while appointed staff better understands the public's concerns and expectations from elected officials and community engagement. Through this collaboration, consensus begins to form and development of the program's framework emerges.

Assumptions:

When reviewing and defining governance structures, jurisdictions should be aware of the following assumptions:

- Government agencies and special districts, such as airports, will often have statutorily defined agency structures and positional authorities that will help define roles and responsibilities for program development and implementation.
- Despite the clearest of role definitions, individuals will often try to influence decisions outside their scope of authority, and these considerations will need to be addressed and/or accommodated.
- There may be statutory or other structural elements that may limit ideal oversight and operational implementation.
- As technology evolves and changes occur within the organization and community, governance structures must be flexible enough to allow for accommodation.

Strategic Objectives:

Agencies deploying video systems should clearly outline the programs' strategic objectives. What are the outcomes the agency is trying to achieve through video deployment? How do the program's objectives align with overall community and organizational goals? Who will monitor outcomes and how will adjustments be made to the program's objectives to respond to changes within the organization and the community?

The needs of video programs are dynamic, and the governance structure developed needs to be able to accommodate the evolution of issues and conditions. Agencies should avoid being in a reactive state, but be able to proactively identify changing conditions and adjust objectives and program requirements in a controlled and deliberate fashion.

Agencies may want to consider a steering committee to help guide overall direction. This committee may become chartered as the governance entity. Video program initiatives often impact multiple disciplines. Various agencies have different video needs, and some video systems may include equipment and staff resources assigned from various agencies. A steering committee can help to build consensus for the program's direction to increase the likelihood that each agency's needs are met. A steering committee also provides a forum where stakeholders can raise issues and where adjustments can be made to overall program direction. If choosing to create such a committee, its role needs to be clearly defined and should not be geared towards providing daily management.

Operational Measures:

The governance structure should include the following operational measures:

- Agencies should identify a program manager who will have daily operational oversight of the video program with clear decision-making authority.
- Roles and responsibilities of other key personnel should also be identified, including reporting relationships.
- Written policies and procedures should be developed to clearly define operational aspects of the program.
- A clearly defined process should be developed to adjudicate concerns between agencies and private sector partners participating in shared video programs.

Technical Measures:

While governance is largely a function of structure and process, some technology measures can bolster governance practices. Those tools are particularly useful in the areas of operational oversight and audit. Technical measures, such as system permissions and controls, can help ensure that governance rules and decisions are being implemented. Additionally, a robust set of automated audit tool features can provide valuable information to the governance structure about compliance with policy and procedural requirements.

Stakeholders:

Program governance requires input and collaboration among a wide array of stakeholders. Each has an interest in the program outcomes and oversight. Agencies developing video programs should engage the following groups:

<u>Internal</u>

- Policymakers;
- Operational users (e.g., first responders, criminal/civil investigators, transportation, public works, etc.); and

- Technical implementers (e.g., information technology, procurement).

External

- Community partners (e.g., business improvement districts, neighborhood associations, etc.);
- Media (identifying issues, providing public awareness, ensuring appropriate oversight); and
- General public (balancing program goals with privacy issues).

Impacts:

Governance is important to the overall performance of video programs and helps to ensure the program's processes will meet the strategic goals of the agencies involved. Governance should provide clear understanding of program goals, lines of authority and communications for all stakeholders and program personnel. The governance framework also ensures that there is sufficient oversight to ensure the appropriate use of video. Finally, a well-defined governance structure should include ways to monitor metrics to measure program outcomes.

CONCLUSIONS

The increasing presence of CCTV video in today's society is widely recognized by government security experts, courts and ordinary citizens. The issue is no longer whether or not government will use video. Instead, the question is how will video be used, managed and governed. The analysis of policy issues in this guidance document is the most recent of the VQiPS program efforts to provide tools for the video system end users (e.g., [1,2,3,4]).

In this document, the VQiPS Working Group Policy Subcommittee has presented a comprehensive framework for policy development. The focus has been to alert decision makers to areas where policy choices must be made. The conclusions of decision makers can and will vary. As one example, some jurisdictions may choose long data retention periods, while others will choose shorter. However, the critical factor is that policy decisions must be made around the issue of video data retention. This document offers such factors for consideration in making policy decisions.

Five overarching substantive issues require consideration across virtually all aspects of a video program: clearly articulated public safety goals; understanding and accommodation of privacy concerns; attention to the security of video networks and data; transparency in the conduct of image collection and data storage and use; and common issues in the operation of public video programs including technology considerations, interoperability and continuity of operation. These issues are discussed in detail in this document.

The Policy Subcommittee identified eight additional issues that require careful consideration by policy makers: 1) sighting and location; 2) access and use, including search; 3) source considerations; 4) notice considerations; 5) monitoring, analysis and analytic applications; 6) retention of data; 7) dissemination of data; and 8) governance. These issues are analyzed according to their underlying assumptions, strategic objectives, operational measures, technical measures, stakeholders, impacts and any other special considerations.

This document offers a flexible tool that can be adapted to the needs of a variety of different jurisdictions and disciplines. It should also be viewed as a living document that can be changed as new policy challenges are identified and new policy solutions are formulated. This document is designed to provide the reader with important issues for government agencies to consider when developing written policies and procedures for the deployment and use of CCTV video systems. It should not be considered a “best practices” or template, but rather a discussion of potentially important policy considerations.

Determining the government purpose(s) for a CCTV video system is essential. A written policy statement outlining public safety purposes and goals is an important step in demonstrating the public safety purpose(s) that government seeks to accomplish. This document should serve as a resource for issues to consider when formulating or updating government policies and procedures for the deployment, use, sharing and maintenance of CCTV video information.

REFERENCES

1. U.S. Department of Commerce Public Safety Communications Research: Video Quality Requirements for Public Safety Users Guide, revised 29 May 2012. Available at http://www.pscr.gov/outreach/vqips/vqips_guide/ (accessed 1 February 2016).
2. U.S. Department of Commerce Public Safety Communications Research: Recommendations Tool for Video Requirements. Available at http://www.pscr.gov/outreach/video/vqips/vqips_guide/use_cases/ (accessed 1 February 2016).
3. U.S. Department of Homeland Security Science and Technology Directorate: Digital Video Quality Handbook, May 2013. Available at http://www.firstresponder.gov/TechnologyDocuments/Digital%20Video%20Quality%20Handbook.pdf (accessed 1 February 2016).
4. U.S. Department of Homeland Security First Responders Group: Optimizing Network Resources for Transmitting Video on Public Safety LTE Networks, March 2015. Available at http://www.firstresponder.gov/TechnologyDocuments/VQiPS%20-%20FY14%20DHS%20Report%20-%20Network%20Optimization.pdf (accessed 1 February 2016).
5. Welsh B, Farrington D, Taheri S: Effectiveness and social costs of public area surveillance for crime prevention. Annual Review of Law and Social Science, 2015, 11:111-130.
6. Massachusetts Emergency Management Agency, Massachusetts Department of Public Health, City of Boston, City of Cambridge, City of Watertown, Massachusetts Bay Transportation Authority Transit Police Department, Massachusetts National Guard, Massachusetts State Police: After Action Report for the Response to the 2013 Boston Marathon Bombings. Available at www.mass.gov/eopss/docs/mema/after-action-report-for-the-response-to-the-2013-boston-marathon-bombings.pdf (accessed 23 March 2016).
7. Garrison D: 5,000 hours of riot video. Evidence Technology Magazine 2012, 10(1):10-14.
8. New York City Police Department: New York City Police Department Releases Draft of Public Security Privacy Guidelines for Public Comment. Available at http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml (accessed 23 March 2016).
9. United States Court of Appeals, Seventh Circuit: Idris v. City of Chicago Illinois, Slip Op. 08-1363 (7th Cir. 2009). Available at http://caselaw.lp.findlaw.com/data2/circs/7th/081363p.pdf (accessed 18 November 2015).

10. *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). Available at https://scholar.google.com/scholar_case?case=9210492700696416594&q=katz+389+347+&hl=en&as_sdt=20000006 (accessed 4 February 2016).
11. *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001). Available at https://scholar.google.com/scholar_case?case=15840045591115721227&q=katz+389+347+&hl=en&as_sdt=20000006 (accessed 4 February 2016).
12. European Union: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995: pages 0031-0050, Luxembourg, 1995. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (accessed 18 November 2015).
13. Information Commissioner's Office: CCTV code of practice. United Kingdom. 2014. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/ (accessed 4 February 2016).
14. Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations, Privacy Commissioner, New Zealand. October 2009. Available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf (accessed 4 February 2016).
15. Constitution Project: Guidelines for Public Video Surveillance. The Constitution Project, Washington D.C., 2007. Available at http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf (accessed 4 February 2016).
16. American Bar Association: Technology-Assisted Physical Surveillance. Criminal Justice Section Standards, Electronic Surveillance: Part B. Available at http://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_taps_toc.html (accessed 4 February 2016).
17. U.S. Department of Homeland Security: CCTV — Developing Privacy Best Practices, Report on the DHS Privacy Office Public Workshop, 17-18 December 2007. Available at https://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf (accessed 4 February 2016).
18. American Public Transportation Association (APTA): Technical Recommended Practice for use of IP cameras in transit related surveillance systems, APTA Standards Development Program, American Public Transportation Association, March 2014. (accessed 4 February 2016).
19. U.S. Department of Defense: Unified Facilities Criteria (UFC) Electronic Security Systems, UFC 4-021-02, October 1, 2013. Available at https://www.wbdg.org/ccb/DOD/UFC/ufc_4_021_02.pdf (accessed 4 February 2016).

20. Savail KL: Implementation of a hybrid analog/digital video management system. ITE District 6 Annual Meeting, Honolulu, Hawaii, June 2006. Available at https://www.sanjoseca.gov/index.aspx?NID=3561 (accessed 22 March 2016).
21. Contestabile J, Patrone D, Babin S: The National Capital Region closed circuit television video interoperability project. J. Emerg. Manag. 2016 Jan-Feb;14(1):31-41. doi: 10.5055/jem.2016.0270.
22. International Association of Chiefs of Police: IACP Technology Policy Framework, January 2014. Available at http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf (accessed 4 February 2016).

APPENDIX

This Appendix contains links to samples of publicly available policies concerning CCTV video usage for public safety by government agencies. The presence of a sample policy in this list should not imply endorsement by VQiPS or DHS.

- Johns Hopkins University: http://pages.jh.edu/security/overview_CCTV.html
- City of Philadelphia Use of Closed Circuit TV Cameras to Monitor Public Rights-of-way: http://www.phila.gov/MDO/Orders%20and%20Directives/Directive%2063%20Use%20of%20CCTV.pdf
- District of Columbia Metropolitan Police Department: http://mpdc.dc.gov/page/cctv-policies-and-procedures
- U.S. National Park Service: http://www.nps.gov/inde/learn/management/upload/RM-9%20Chapter%2026-CCTV.pdf
- State of Vermont Guidelines for the Use of Video-Monitoring Equipment in, upon, and around State Facilities: http://bgs.vermont.gov/adminpolicies/policy22
- University of Pennsylvania CCTV Monitoring and Recording of Public Areas for Safety and Security Purposes Policy: http://www.upenn.edu/almanac/volumes/v59/n09/cctv.html