Privacy Impact Assessment
for the

Reality Mobile Kentucky: Operational Field Test

October 24, 2008

Contact Point
K. Phil Waters
Department of Homeland Security
Science and Technology Directorate
(202) 254-6766

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Reality Mobile Kentucky project is a research and development effort in the DHS Science & Technology Directorate (S&T) that seeks to test the operational effectiveness and efficiency of streaming video for law enforcement applications. Reality Mobile software is a commercially available software-driven system that would allow first responders and law enforcement officials to send and receive live video and geospatial coordinates. S&T is conducting this PIA because the Kentucky State Police will capture images of individuals during the field test in accordance with their law enforcement authorities, standard operating procedures, and applicable state and local laws. This PIA covers only the research activities conducted by S&T during this operational field test. Should S&T acquire the technology and transition it to a DHS Component, that DHS Component will be responsible for completing the subsequent privacy assessments of the Reality Mobile technology and its use.

Overview

The Reality Mobile system would allow first responders and law enforcement officials to send and receive live video and geospatial coordinates, view video from fixed or mobile cameras (including cameras built into handheld devices like cell phones), and receive images from a field command post via cell phones (the cell phones will not store the images). The key to the Reality Mobile system is its server application that can distribute both the video client software and the streaming video to the hand-held devices.

Title 3 of the Homeland Security Act assigns S&T the responsibility for conducting research in support of the Department's mission. Under Subchapter 3 §182, "the Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department."

The Reality Mobile Kentucky project will support S&T's research mission by testing the operational validity of streaming video for first responders and law enforcement applications. The objectives of the project are (1) to test the system's functionality (connectivity, features, and ergonomics); and (2) to test the integration of the prototype in real-world first responder and law enforcement missions such as all-points bulletins, Amber Alerts, identification of suspicious packages, and emergency situations requiring situational awareness. These research activities will help S&T evaluate the utility of this technology on behalf of its potential customers and determine how first responders and law enforcement personnel might integrate the technology into their operations.

To determine the benefits and utility the technology offers law enforcement personnel, S&T will provide funding to Oak Ridge National Laboratory to conduct an operational field test of this technology in partnership with the Kentucky State Police. The field test will focus on establishing the benefits of deploying Reality Mobile technology in an operational environment, determing the Reality Mobile product's ability to meet urgent needs of the first responder community, and assessing the technology's impact on real-time situational awareness at the Kentucky Intelligence Fusion Center (KIFC), which is operated by the Kentucky State Police (KSP). Upon completion of

this field test, S&T will determine whether the Reality Mobile technology could benefit DHS operational Components or other S&T customers.

During this field test, the Reality Mobile system will be deployed by the Kentucky State Police. A limited number of officers (a maximum of 20) will receive cell phones that are equipped with the Reality Mobile system and able to both send and receive video and text information. During the test, Kentucky State Police will use the system during law enforcement actions in support of active cases and investigations. The Reality Mobile Management Console will reside at the State Police headquarters and will be programmed with the ability to exchange real time video and data between the on-scene officer, the Kentucky State Police headquarters, and the Kentucky State Intelligence Fusion Center. All images and other personally identifiable information collected during the field test will be maintained, owned, and under the control of the Commonwealth of Kentucky. S&T will not have access to any personally identifiable information collected or generated during this field test. S&T will only have access to non-personally identifiable information related to the effectiveness of the system.

The Reality Mobile testing will include the following participants

1. Agencies from the Commonwealth of Kentucky (including the Kentucky Homeland Security Office, Kentucky Intelligence Fusion Center, and state and local law enforcement officers) will evaluate the usefulness of the product in conducting routine law enforcement operations and during emergency situations.

2. Oak Ridge National Laboratory (ORNL) will serve as the system integrator and provide technical support for the installation and system integration of the Reality Mobile capabilities into the Kentucky Intelligence Fusion Center.

3. S&T Program Managers will participate as observers in some portions of the field tests. These portions will not include active law enforcement activities involving entrance into people's homes. However, these personnel will not have access to any personal identifiable information or Law Enforcement Sensitive data. Their participation will strictly be to observe and evaluate the functionality, practicality, and effectiveness of the technology in an operational environment.

The Reality Mobile technology was successfully tested in the lab environment at ORNL in a 90-day demonstration, and now, through this phase of research and development, will be tested in the field by the Kentucky State Police under realistic conditions to assess (1) whether the product actually performs as advertised in the field, (2) whether the product allows the KSP to perform their responsibilities better, more efficiently, faster, or adds capabilities, and (3) whether the product is cost effective for S&T's customer—the law enforcement community.

This PIA covers only S&T's research and development process. Should any DHS Component or other Federal agency acquire the Reality Mobile technology, that agency would conduct a separate PIA to cover operational use.

Section 1.0 The System and the Information Collected and Stored Within the System

1.1 What information is to be collected?

The System's Technology Enables It to Record:

- ☒ **Video**
  - Static Range: *Approximately 50 feet*
  - Zoom Range: *Approximately 1,000 feet*
- ☒ **Tracking**
  - ☐ Automatic (for example, triggered by certain movements, indicators)
  - ☒ **Manual** (controlled by a human operator)
- ☐ Sound
  - Frequency Range:

The System Typically Records:

- ☒ **Passersby on public streets**.
  During the course of their law enforcement duties, the Kentucky State Police will collect images of members of the public in accordance with their standard operating procedures and applicable state and local laws.
- ☒ **Textual information** (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
- ☒ **Images not ordinarily available to a police officer on the street**:
  - ☒ Inside commercial buildings, private homes, etc.
  - ☒ Above the ground floor of buildings, private homes, etc.

  All uses of this technology by Kentucky State Police officers will be limited to the scope of their authorities to collect images and conduct surveillance during the course of performing law enforcement duties. If a Kentucky State Police officer has the Reality Mobile-equipped phone streaming video and enters a building while the cell signal is still available, the video showing the interior of the building will be streamed out. An officer must be present with a phone that he or she has activated or allowed to be activated for the video to be streamed.

1.2 From whom is the information collected?

- ☒ **General public in the monitored areas.**
  Since many law enforcement activities occur in public areas, if the phone is streaming video in the public area, persons other than those of interest may be captured by the video stream.
- ☒ **Targeted populations, areas, or activities (please describe).**
  Individuals who are persons of interest in law enforcement activities.
- ☐ Training included directives for program officials to focus on particular people, activities, or places (please describe).

1.2.1 Describe any training or guidance given to program officials that directs them to focus on particular people, activities, or places.

The law enforcement officials participating in this project will be instructed to limit recording images and video only as permissible by applicable state and local laws and pursuant to their own regulations during the course of their law enforcement duties. The training will include specific reference to the fact that this is a research effort using new technology and how they will ensure their laws and regulations will be enforced within the research context.

1.3 Why is the information being collected?

☐ Crime prevention
☐ To aid in criminal prosecution
☐ For traffic-control purposes
☐ Terrorism investigation
☐ Terrorism prevention
☒ **Other (please specify) –**

The purpose of this project is to test the Reality Mobile technology in an operational environment and assess the impact of the resultant improvements to information sharing and situational awareness. The Reality Mobile technology will be tested to determine (1) whether the product actually performs as advertised in the field, (2) whether the product allows the KSP to perform their responsibilities better, more efficiently, faster, or adds capabilities, and (3) whether the product is cost effective. The capability of the Reality Mobile system to share streaming video and images instantaneously between team members in the field and headquarters will likely translate to quicker response times in situations routinely encountered by first responders and law enforcement officials. Since this is an operational test, law enforcement officials may use the video as part of active case files in pursuit of law enforcement activities.

1.3.1 Policy Rationale

☒ **A statement of why surveillance cameras are necessary to the program and to the governmental entity's mission.**

S&T's mission is to conduct basic and applied research, development, demonstration, testing, and evaluation activities to support all elements of DHS. The Reality Mobile system research is testing a technology that would support the DHS mission of preventing criminal and terrorist acts by facilitating the instantaneous transmission of valuable operational information (i.e. images of terrorist/criminal suspects, images of emerging emergency situations, transmission of images of suspected explosive or unknown devices). No specific operational applications have been finalized. The greatest benefit of the system is the ability to quickly share information among law enforcement members regardless of location. This capability

may be leveraged in a variety of ways including remote identification of suspicious people and as a situational awareness application during an emergency situation.

- ☐ Crime prevention rationale: (for example, crimes in-progress may only be prevented if the cameras are monitored in real-time. Or, a clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)
- ☐ Crime investigation rationale: (for example, a hidden camera may be investigative but not preventative, providing after-the-fact subpoenable records of persons and locations.)
- ☐ Terrorism rationale: (for example, video images are collected to compare to terrorist watch lists.)

1.3.1.1 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features are necessary to advance the governmental entity's mission. For example, describe how low-light technology was selected to combat crime at night. It is not sufficient to merely state the general purpose of the system.

The capability for live, streaming-video via a quick and robust connection with operations headquarters may enhance the situational awareness of law enforcement and first responders in the field. The Reality Mobile Kentucky field test will assess the impact of the application of live streaming-video in routine law enforcement activities to determine how potential S&T customers might benefit from this technology.

1.3.1.2 It would be adequately specific, for example, to state that cameras which are not routinely monitored provide after-the-fact evidence in criminal investigations by providing subpoenable records of persons and locations. Similarly, it would appropriate to state, for example, that video images are collected to compare to terrorist watch lists and wanted persons lists.

Live streaming video could be used to facilitate the instantaneous transmission of valuable operational information between a headquarters facility and law enforcement officers or agents in the field. S&T is funding ORNL to conduct the field test in order to evaluate the operational utility of this capability for S&T customers.

1.3.1.3 How is the surveillance system's performance evaluated? How does the government assess whether the surveillance system is assisting it in achieving stated mission? Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

The Kentucky law enforcement entities do not currently possess a system that shares live, streaming video. The purpose of this research is to determine whether the technology would enhance the capability of law enforcement officials and first responders to carry out their daily missions. When this research is completed, the Commonwealth of Kentucky will provide S&T with a qualitative evaluation of the performance of and effectiveness to meet routine and emergency operations. This evaluation will be based upon (1) whether the product actually performs as advertised in the field, (2) whether the product allows the KSP to perform their responsibilities better, more efficiently, faster, or adds capabilities, and (3) whether the product is cost effective.

1.3.2 Cost Comparison

Please describe the cost comparison of the surveillance system to alternative means of addressing the system's purposes.

At present, there is no comparable system against which the cost of the Reality Mobile system could be evaluated.

1.3.3 Effectiveness

☒ **Program includes evaluation of systems performance (please describe how performance is evaluated.)**

The Commonwealth of Kentucky will provide S&T with a qualitative evaluation of the effectiveness of the Reality Mobile system based on (1) whether the product actually performs as advertised in the field, (2) whether the product allows the KSP to perform their responsibilities better, more efficiently, faster, or adds capabilities, and (3) whether the product is cost effective.

☐ Evaluation includes metrics to measure success (for example, crime statistics.)

☐ Program includes a timeline for evaluation

1.4 How is the information collected?

☐ Real-time monitoring, with images streamed, but not stored.

☒ **Real-time monitoring with images stored.**

The Kentucky State Police will store and retain the images and video in accordance with applicable state and local laws.

☐ Images not monitored, only stored.

1.4.1 Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

S&T will not have access to the images that Kentucky State Police will collect during the field test, and thus, will not store, delete, alter, or enhance the images.

The Commonwealth of Kentucky will be the sole custodian of all images and other PII collected during the field test and will control access to and manage the information in accordance with applicable state and local laws.

1.5 What specific legal authorities, arrangements, and/or agreements defined the surveillance system?

☒ **Legislative authorization at the city or state level**

The Homeland Security Act (Federal legislation) authorizes S&T to conduct this research.

The Kentucky State Police are authorized to collect images and conduct surveillance during the course of performing law enforcement duties. The collection and retention of the images and videos will be limited to these authorities and will not be expanded based on the specific capabilities or particular uses of this technology.

☐ Executive or law enforcement decision
☐ Decision-making process included public comment or review
☐ Entity making the decision relied on:
- ☐ case studies
- ☐ research
- ☐ hearings
- ☐ recommendations from surveillance vendors
- ☐ information from other localities
- ☐ other (please specify)

Funding:

☐ DHS Grant
☐ General revenues
☐ Law enforcement budget
☐ Other (please specify)
☐ Funding has limited duration (please specify)
☒ **Funding renewal is contingent on program evaluation**

Appendix is attached, including:

- ☒ **S&T authorizing legislation**

- ☐ Grant documents
- ☐ Transcript of public hearing or legislative session
- ☐ Press release
- ☐ Program manuals outlining the system's rules and regulations
- ☐ Other (please specify)

1.5.1 The section should also include a list of the limitations or regulations controlling the use of the video surveillance system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

The system will be used in a multitude of real-world law enforcement situations which cannot be uniquely identified since some will occur spontaneously. The Kentucky State Police view the streaming video from the Reality Mobile phones as a similar capability to that which is routinely available from in-car mounted cameras. The Kentucky State Police will comply with all applicable state and local laws in utilizing the Reality Mobile system during the field test. This means that during the actual test, the Kentucky State Police will assess the new technologies being tested, and the way those technologies will be used, and ensure that all uses conform to all applicable laws, regulations and policies.

1.6 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use discuss what privacy risks were identified and how they were mitigated. If during the system design or technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks include:

- ***Privacy rights****. For example, the public cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, Alcoholics Anonymous, or social, political or religious meeting.*
- ***Freedom of speech and association****. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or the associations between individuals. This may chill constitutionally-protected expression and association.*
- ***Government accountability and procedural safeguards****. While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, creating a system of accountability for all uses.*
- ***Equal protection and discrimination****. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, for example, profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.*

The Kentucky Reality Mobile system will test the relevance and application of live steaming video in routine law enforcement activities to determine how law enforcement agents and agencies would benefit from this technology. The Commonwealth of Kentucky will be the sole custodian of all images and other PII collected during the field test, and will manage the information in accordance with applicable state and local laws. The information may become case data and may be retained per existing Kentucky state guidelines for video images.

The privacy risk associated with this field test is that images of individuals may be captured without their knowledge and consent, that those images may be used inappropriately to support prosecution of a crime, and that the images may be viewed by unauthorized personnel. To mitigate these risks, all personnel capturing video during the field test will be trained law enforcement officers. Video images and other PII collected during the project will be collected, stored, and retained in accordance with Kentucky state law enforcement authorities and applicable state and local laws.

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the information derived from the video cameras.

Please describe the routine use of the images. If possible, describe a situation (hypothetical or fact-based, with sensitive information excluded) in which the surveillance cameras or technology was accessed for a specific purpose.

S&T is funding the field test to evaluate the operational utility of streaming video for law enforcement agents and agencies. During the field test, the Kentucky State Police will use the system on a daily basis in support of criminal investigations and prosecutions.

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that information is handled in accordance with the above described uses. For example, is appropriate use of video covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the video technology or records?

The Kentucky State Police must comply with all applicable state and local laws governing the collection of video images. This means that all locations and all manners in which the Kentucky State Police use this new technology will be reviewed and determined to comply with all applicable state and local laws. All personnel capturing and otherwise using the images and video during the field test will be trained and authorized law enforcement officers and will be subject to Kentucky State Police policies and disciplinary actions. Any information that would be used to prosecute an individual for a crime would be evaluated by court officials for admissibility.

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the images in the system (i.e., how long are images stored)?

☐ 24-72 hours
☐ 72 hours – 1 week
☐ 1 week – 1 month
☐ 1 month – 3 months
☐ 3 months – 6 months
☐ 6 months – 1 year
☐ more than 1 year (please describe)
☒ **In accordance with applicable laws, regulations, and procedures.**

S&T will not have access to, retain, or store any images or other PII obtained during this field test. However, the information collected by the Kentucky State Police during the field test would become part of case files and be retained in accordance with Kentucky State Police policies and procedures or as required by applicable state and local laws.

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

None.

3.2 Retention Procedure

☐ Images automatically deleted after the retention period expires
☒ **System operator required to initiate deletion**
☐ Under certain circumstances, officials may override detention period:
  ☐ To delete the images before the detention period
  ☐ To retain the images after the detention period
  ☐ Please describe the circumstances and official process for override

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the indicated period.

S&T will not have access to, retain, or store any information collected during the field test. The Kentucky State Police will retain information relevant to criminal cases in accordance with Kentucky State Police policies and state and local laws.

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the surveillance operation, such as various units or divisions within the police department in charge of the surveillance system. *External sharing will be addressed in the next section.*

4.1 With what internal entities and classes of personnel will the information be shared?

Internal Entities

☐ Investigations unit
☐ Auditing unit
☐ Financial unit
☐ Property-crimes unit
☐ Street patrols
☐ Command unit
☒ **Other (please specify)**
☐ None

S&T will not have access to or share the information. The Kentucky State Police will share the information within their organization only as appropriate or required by law in order to pursue criminal investigations and prosecutions.

Classes of Personnel

☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☒ **Other (please specify)**

Only personnel directly authorized by the Commonwealth of Kentucky will have access to the information.

4.2 For the internal entities listed above, what is the extent of the access they receive (i.e. what records or technology is available to them, and for what purpose)?

Internal personnel will have access to streaming-video received via commercially procured cell phones. The commercial cell phones will not store the video images.

4.2.1 Is there a written policy governing how access is granted?

☐ Yes (please detail)
☒ **No**
☒ **Other**

While S&T will not have access to or be authorized to grant access to this data. The Kentucky State Police will grant access to the data pursuant to standard law enforcement procedures and applicable state and local laws. These written rules

and any other written policy will be specifically identified and made part of the governance process and documentation for the research effort.

4.2.2 Is the grant of access specifically authorized by:

☐ Statute (please specify which statute)
☐ Regulation (please specify which regulation)
☒ **Other (please describe)**
☐ None
Access to the data must be specifically authorized by the Kentucky State Police.
.

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

☒ **Off-site, from a remote server**
☐ Via copies of the video distributed to those who need it
☐ Only by viewing the video on-site
☐ Other (please specify)
The test will include personnel operating a single remote server which will centralize the receipt and dissemination of test images. Images related to the test period will be routed to a specific server and are accessible only to authorized law enforcement personnel.

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

A privacy risk associated with the Reality Mobile system is that images collected during the field test will be shared with unauthorized personnel. To mitigate this risk, only the Kentucky State Police will have access to or the authority to grant access to the information. All personnel collecting images and video during the field test will be trained law enforcement officers and will comply with all applicable state and local laws.

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including federal, state and local government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the images or information about the images is or will be shared. The term "external entities" refers to individuals or groups outside your organization.

☐ Local government agencies (please specify)
☒ **State government agencies (please specify)**
The Kentucky State Police will be the sole custodian of the images/information collected during the field test. The Kentucky State Police will share the information will state agencies as appropriate or required by law for criminal investigations and prosecutions. S&T will not have access to, and will not have the authority to grant access to, any images or PII collected during the field test.
☐ Federal government agencies (please specify)
☐ Private entities:
- ☐ Businesses in monitored areas
- ☐ Insurance companies
- ☐ News outlets
- ☐ Other (please specify)

☐ Individuals:
- ☐ Crime victims
- ☐ Criminal defendants
- ☐ Civil litigants
- ☐ General public via Public Records Act or Freedom of Information Act requests
- ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe:

- ☐ The purpose for disclosure-
- ☐ The rules and regulations governing disclosure
- ☐ Conditions under which information will not be disclosed
- ☐ Citations to any specific authority authorizing sharing the surveillance images

Purpose: The purpose of this project is to test the functionality of the Reality Mobile technology in an operational environment and assess the impact of the resultant improvements to information sharing and situational awareness. The Kentucky State Police will use the system during law enforcement actions in support of active cases and investigations. The capability of the system to share streaming video and images instantaneously between team members in the field and headquarters will likely translate to quicker response times and better prevention of, and protection from, emergency situations.
Rules & Regulations: S&T does not have access to and cannot disclose to any party the images or other information collected during the field test. The Kentucky State Police will disclose the information to state government agencies as appropriate to support criminal and civil investigations and prosecutions.
Disclosure: S&T does not have access to and cannot disclose to any party the images or other information collected during the field test. The Kentucky State Police will not disclose the images or information collected during the field test to any individual other than an authorized law enforcement officer or court official.

Authority: S&T does not have the authority to access or share the surveillance images. The Kentucky State Police will share the images to support criminal investigations and prosecutions in accordance with and as required by state and local laws.

5.3 How is the information transmitted or disclosed to external entities?

☐ Discrete portions of video images shared on a case-by-case basis
☐ Certain external entities have direct access to surveillance images
☐ Real-time feeds of images between agencies or departments
☒ **Images transmitted wirelessly or downloaded from a server**
☐ Images transmitted via hard copy
☒ **Images may only be accessed on-site**

Video information is transmitted over a commercial cellular service, over a mobile switching center dedicated to Commonwealth of Kentucky operations. The images are then stored at the Kentucky Intelligence Fusion Center, a secure facility with access control and information security measures compliant with state and local laws.

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with any external organization(s) with whom information is shared, and does the MOU reflect the scope of the information currently shared?

☐ Yes
☒ **No**

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☒ **One person is in charge of ensuring the system remains secure during the information sharing (please specify)**
Kentucky State Police Information Systems Manager
☐ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☐ Technological protections do not remain intact once information is shared

The Kentucky State Police will secure the information in accordance with applicable state and local laws and policies. All data collected during the field test will be maintained, owned, and stored by and under the sole control of the Commonwealth of Kentucky. The data shall be stored in a secure facility with access control and information security

measures compliant with state and local laws.

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your department/agency?

The privacy risk is that unauthorized personnel could gain access to the images. To mitigate that risk, the images will not be stored on the individual cell phones utilized during the field test and the captured images will only be retained on the Kentucky State Police server in the KIFC, which is accessible only to authorized law enforcement personnel.

Section 6. 0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Command staff
☐ Shift commanders
☐ Patrol officers
☐ Persons outside the organization who will have routine or ongoing access to the system (please specify)
☒ **Other (please specify)**

Images will not be altered or enhanced after the field test, and only authorized officials and users designated by the Commonwealth of Kentucky shall have access privilege to the collected data.

6.1.1 Are different levels of access granted according to the position of the person who receives access? If so, please describe.

☒ **All authorized users have access to real-time images**

Only the Commonwealth of Kentucky will have daily access to the collected data. ORNL representatives will review logs to establish the overall use of the system and will work under the auspices of the Commonwealth of Kentucky to establish procedures to evaluate the quality of video. Under no circumstances will ORNL remove collected data from the Kentucky Intelligence Fusion Center. ORNL will not have access to images or other PII; ORNL is only supporting setup and basic operation of the system. ORNL analysis is only performance monitoring, not data monitoring.

☐ Only certain authorized users have access to real-time images (please specify which users)
☒ **All authorized users have access to stored images**
☐ Only certain users have access to stored images (please specify which users)
☐ All authorized users can control the camera functions (pan, tilt, zoom)
☐ Only certain authorized users can control the camera functions
☐ All authorized users can delete or modify images

☐ Only certain authorized users can delete or modify images (please specify which users)

6.1.2 Are there written procedures for granting access to users for the first time?

☐ Yes (please specify)
☒ **No**

6.1.3 When access is granted:

☐ There are ways to limit access to the relevant records or technology (please specify)
☒ **There are no ways to limit access**

S&T has no mechanism for limiting access to the data. The Kentucky State Police will have the sole authority for granting/limiting access to the records and the technology.

6.1.4 Are there auditing mechanisms:

☐ To monitor who accesses the records?
☐ To track their uses?

The Reality Mobile software does not track which users have access to which real time or stored video. The Kentucky State Police would develop and implement any such auditing mechanisms in accordance with applicable state and local laws.

6.1.5 Training received by prospective users includes discussion of:

☐ Liability issues
☐ Privacy issues
☒ **Technical aspects of the system**
☐ Limits on system uses
☐ Disciplinary procedures
☐ Other (specify)
☐ No training

The training lasts:

☐ None
☒ **0-1 hours**
☐ 1-5 hours
☐ 5-10 hours
☐ 10-40 hours
☐ 40-80 hours
☐ More than 80 hours

The training consists of:

☐ A course
☐ A video
☐ Written materials

☐ Written materials, but no verbal instruction
☐ None
☒ **Other (please specify)-**
Reality Mobile will provide technical training on the system via verbal instruction.

6.2 The system is audited:

☐ When an employee with access leaves the organization
☐ If an employee is disciplined for improper use of the system
☐ Once a week
☐ Once a month
☐ Once a year
☐ Never
☒ **When called for**
The Kentucky State Police will audit their records as required by their existing law enforcement procedures and applicable state and local laws.

6.2.1 System auditing is:

☐ Performed by someone within the organization
☐ Performed by someone outside the organization
☐ Overseen by an outside body (for example a city council or other elected body – please specify)
N/A

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

The privacy risk is that an unauthorized user would gain access to the information or that an authorized user would use the information for an unauthorized purpose. To mitigate these risks, the system server will be located in a secure controlled space which is manned 24 hours per day and access to the data will be restricted to authorized members of the Kentucky State Police.

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of video recording that they are within view of a surveillance camera?

☐ Signs posted in public areas recorded by video cameras
☐ Signs in multiple languages
☐ Attached is a copy of the wording of such notice signs
☒ **Notice is not provided**
S&T will not provide notice to individuals of video surveillance. The Kentucky State Police will provide notices as required by applicable state and local laws.
☐ Other (please describe)

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the video surveillance system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

☐ Yes
☒ **No**
No competing software is currently available for comparison.

8.2 What design choices were made to enhance privacy?

☐ The system includes face-blurring technology
☐ The system includes blocking technology
☐ The system has other privacy-enhancing technology (Please specify)
☒ **None (Please specify)**
The purpose of this trial is to research and actualize the needs of the state and local law enforcement community for the possible future application of this technology. The research effort is designed to ensure that all uses of the technology, images, and video will be pursuant to the state and local laws as well as all applicable regulations governing the Kentucky State Police and any other government entity participating in the test.

Responsible Officials

K. Phil Waters
Department of Homeland Security
Science and Technology Directorate

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX A: Legal Authorization

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.