Privacy Impact Assessment
for the

RealEyes Project

July 21, 2008

Contact Point
John Price
Department of Homeland Security
Science and Technology Directorate
(202) 254-5662

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

Abstract

RealEyes is a research and development project in the DHS Science & Technology Directorate (S&T) that seeks to test the operational effectiveness and efficiency of streaming video for first responders and law enforcement applications. RealEyes is a prototype software system that would allow first responders and law enforcement officials equipped with Personal Digital Assistants (PDAs) to send and receive live video and geospatial coordinates, view video from fixed or mobile cameras, and receive data (video, photos and text) from a field command post using basic cellular technology. S&T is conducting a PIA because a planned phase of technology testing may involve incidentally capturing images of individuals who are not volunteer participants in the research effort. This PIA covers only the activities conducted during the testing phase of the RealEyes project. If the RealEyes technology is deployed into operational use, the DHS Component implementing the technology will be responsible for completing any subsequent privacy assessments of the RealEyes technology and its use.

Overview

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 RealEyes 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 RealEyes project are (1) to test the system's functionality (connectivity, features, and ergonomics); and (2) to test the integration of the RealEyes prototype in scenarios that duplicate 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. Federal Law Enforcement agencies contain unique divisions with specific missions that must individually evaluate how the RealEyes technology can best be utilized for their purposes. For example, a bombing prevention team will evaluate the efficiency and clarity of the enhanced communication capability provided by RealEyes with respect to their specific mission. A Federal Law Enforcement agency is the only current intended customer of the RealEyes technology and will be involved in all of the testing situations. Other federal DHS component representatives may be present at the testing to observe the technology, but specific testing for other component needs is not in the scope of this particular effort. These research activities will help S&T and its potential customers evaluate the utility of this technology and determine how first responders and law enforcement personnel might integrate the RealEyes technology into their operations.

RealEyes is a prototype software-driven system that 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 PDAs), and receive images from a field command post via PDAs (the PDAs will not store the images). The key to RealEyes is its server application that can distribute both the video client software and the streaming video to the hand-held devices.

The RealEyes testing will include the following participants:

1. S&T Program Manager: The S&T Program Manager will perform program management and oversight and will coordinate the testing project including overseeing participation of the additional participants described below (the Federal Law Enforcement Agency) who will assist in designing and reviewing the research scenarios that are relevant to their mission and operational needs, and the Industry Performer who will provide technical support to the research project). The S&T Program Manager will have access to the live feed images on site with the participating Federal Law Enforcement Agency volunteers and on the laptop that will serve as the command center for purposes of the field test and that will receive the video feeds from the field volunteers.

2. Federal Law Enforcement Agency: In order to test the system, volunteer Federal employees from the Federal Law Enforcement Agency will conduct scenario-based testing to assess whether RealEyes would be suitable for operational needs. The volunteers will have access to the live feed images transmitted via PDAs. The Federal Law Enforcement Agency is S&T's first intended customer of the final operational implementation of RealEyes, with the potential to use this system for operational needs such as Amber Alerts. While the Federal Law Enforcement Agency may use this technology in operations in the future, the current focus of this research effort is to determine whether this new capability *could* be useful in an operational environment. The actual decision *whether* to use RealEyes technology in operations will be made later, after the research effort concludes.

3. Industry Performer: The industry performer developed the RealEyes technology and will provide on-site technical and logistical support. The industry performer will temporarily place all images utilized during the testing phase on their private server. This server is separated from the rest of their network, is behind a firewall, and is password protected. The images associated with this effort are protected with 128-bit encryption. The industry performer will have access to the live feed images and the captured images for the length of the testing period and 24 hours following its conclusion. This short retention period will allow a small window of follow-up after the testing period, so that the industry performer has adequate time to address comments and issues raised during the test. At the end of the 24-hour period, the industry performer will send an email confirmation to the Federal Law Enforcement Agency and S&T project managers that the images have been deleted from the server.

The RealEyes technology was successfully tested in the lab environment and now, through this phase of research and development, will be tested in the field in various operational settings, in a variety of locations significant to the Federal Law Enforcement Agency's operations, and under realistic conditions to verify suitability for S&T's intended customers, the law enforcement and first responder communities.

This PIA covers only S&T's research and development process. Should the Federal Law Enforcement Agency or any other Federal agency acquire the RealEyes 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.**
  This project will involve capturing images via live streaming video of Federal Law Enforcement Agency volunteers. Research participants (S&T, the Federal Law Enforcement Agency, industry performers – see above descriptions) will make every effort to confine the captured images to volunteers from the Federal Law Enforcement Agency. However, it is possible that incidental images of passers-by could be inadvertently captured in the background of the images of volunteers during the research scenarios. DHS will not retain any of the streamed images, whether of volunteers or unintended bystanders, beyond the 24-hour period described in the introduction.
- ☐ 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.

1.2 From whom is the information collected?

- ☐ General public in the monitored areas.
- ☒ **Targeted populations, areas, or activities (please describe).**
  Research participants (this term refers to volunteers from the Federal Law Enforcement Agency, S&T project management team, and industry performer representatives) will capture images of volunteers from the Federal Law Enforcement Agency participating in the project. However, the research

participants could inadvertently capture incidental images of passers-by in the background.

☐ 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.

All participants in this project will be instructed to capture only images of volunteer federal employees acting as test subjects and to make every effort to avoid capturing images of passers-by.

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 functionality of the RealEyes technology in the intended customer's (a Federal Law Enforcement Agency) operational environment and assess the impact of the resultant improvements to information sharing and situational awareness. No specific Federal Law Enforcement Agency operation plans have been established. Developing plans will be one of the intended outcomes of this research effort. The capability of the RealEyes 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.

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 RealEyes research is testing a technology that would support the Federal Law Enforcement Agency's mission of securing America from both criminal and terrorist acts by facilitating the instantaneous transmission of valuable operational information to field agents (i.e. images of terrorist/criminal suspects, images of emergency situations, transmission of images of suspected explosive or unknown devices). The testing periods will aid the Federal Law Enforcement Agency in determining how best to utilize the RealEyes system. No specific operational applications have been finalized. The greatest benefit of the system is the ability to quickly share information among team members regardless of location. This capability may be leveraged in a variety ways including remote identification of

suspicious objects 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 agents and first responders in the field, allowing them to be better prepared for emergency situations. The RealEyes project will test the application of live streaming video in various scenarios (casualty evacuations, tracking of suspects, hazardous materials, etc.) to determine how agents and agencies would 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 Federal Law Enforcement Agency field agents. The video utilized for the testing period will be images of the industry performer, S&T program management, or the Federal Law Enforcement Agency program management volunteers. Each field volunteer will have a PDA equipped with a camera. The PDAs will record video of the volunteers and transmit video back to the command center (here, a laptop equipped with the Real Eyes server software). The operators of the command center laptop will decide which videos will be shared with the volunteers as either an optional video they can select to watch or as a video override which will play the video on all of the PDAs. The videos will be only utilized during the course of the testing period and will not be saved on the PDAs.

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 Federal Law Enforcement Agency and other law enforcement entities do not currently possess a system that shares live, streaming video. The purpose of this research is to determine whether the RealEyes technology would enhance the capability of law enforcement officials and first responders to carry out their missions. When this research is completed, S&T and the Federal Law Enforcement Agency will provide a qualitative evaluation of the performance of RealEyes based on the unique mission needs and the outcome of the testing.

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 RealEyes could be evaluated.

1.3.3 Effectiveness

☒ **Program includes evaluation of systems performance (please describe how performance is evaluated.)**
S&T and the Federal Law Enforcement Agency will provide a qualitative evaluation of RealEyes with respect to their missions based on the information acquired during the testing period.
☐ 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 images will be stored on a single server for a maximum period of 24 hours.
☐ 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?

Images utilized during the testing period will be stored on a single remote server for a period no longer than 24 hours. During this period, images may be accessed by the industry performer project manager and IT manager so that the industry performer has adequate time to address comments and issues raised during the test, but images cannot be altered or enhanced. After 24 hours, all images will be destroyed.

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. Federal legislation also provides explicit authorization to the Federal Law Enforcement Agency to collect this information.
☐ 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:
- ☒ **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?

DHS will require participants in this research project to take all possible measures to avoid capturing images of individuals not involved in the RealEyes testing. Additionally, the testing will limit the time that images are stored to less than 24 hours.

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 RealEyes project will test the relevance and application of live streaming video in mock operational scenarios. The project will use volunteers from the Federal Law Enforcement Agency in public settings - conditions that approximate law enforcement situations. The RealEyes project scenarios will take place in several different public venues (streets, airports, train stations, ports, etc.) for brief time periods (typically less than 5-8 hours). The prototypes used in this project are not fixed and are not fixed camera systems that passively collect images for indefinite periods of time. The RealEyes prototypes are handheld PDAs equipped with cameras carried by test subjects who are attempting to capture images of other test subjects.

The privacy risk associated with the RealEyes research project is that images of passers-by could inadvertently be captured by S&T without the knowledge or consent of those individuals. To mitigate this risk, all research participants will be instructed to make every effort to avoid capturing images of passers-by. The latest software upgrade to the industry performer's technology has also implemented 128-bit encryption. The images will not be stored on the PDAs; therefore, research participants will not have access to the images they capture. Images will be retained on the industry performer's server for 24 hours so that the industry performer has

adequate time to address comments and issues raised during the test, after which they will be deleted.

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 will only use the images to test the operational validity of streaming video for the Federal Law Enforcement Agency's operations. A sample Federal Law Enforcement Agency use of the technology would be to transmit an image of an individual wanted for questioning by law enforcement to Federal Law Enforcement Agency field agents. (The Federal Law Enforcement Agency would conduct a separate PIA to cover operational use of this system. This PIA covers only S&T's research and development process for the Federal Law Enforcement Agency.)

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?

All personnel involved in the RealEyes project will be instructed to minimize the image capture of individuals who are not associated with testing. Images will not be stored on the PDAs used in the testing; therefore, the research participants will not have access to the images. The images will be stored on the industry performer's server for 24 hours for post-testing period evaluation, after which they will be destroyed.

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)
- ☐ indefinitely

The images utilized during the testing will be retained for a maximum of 24 hours on a server belonging to the industry performer utilized during the test period. The industry performer, the Federal Law Enforcement Agency's project management team, and DHS S&T project management team need this short retention period to revisit the testing conditions if any immediate questions about the technology's abilities arise during and after the test. The individual Personal Digital Assistants (PDAs) utilized during the testing will not retain the images.

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

There will not be any exemptions for the retention period.

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.

The industry performer will retain the images on its server for a maximum period of 24 hours, after which the images will be destroyed. This time period allows research participants and the industry performer adequate time to address comments made during the course of the testing event.

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

During the testing phase of this R&D project, the volunteer Federal Law Enforcement Agencytest subjects and the DHS S&T project management team will have access to the information via live feed. It is possible that representatives of other DHS components may attend a testing period to passively observe the scenario. The purpose of this observation would be to evaluate whether or not the RealEyes technology might be useful for those components. These representatives would not be active participants and would not have access to the information transmitted during the testing period.

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

The volunteer Federal Law Enforcement Agency test subjects, the Federal Law Enforcement Agency program manager, and S&T project management staff will only have access to information during the testing period as images are disseminated. The PDAs will not store images and the volunteers will not have access to the images stored on the server for the 24 hour period.

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 PDAs. The PDAs will not store this information. The industry performer will delete the images from their server after 24 hours.

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

☐ Yes (please detail)
☒ **No**

The volunteer Federal Law Enforcement Agency test subjects and the S&T project management team are the only internal groups that will have access to the images via live feed. No other internal personnel will be granted access to the images.

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

The Federal Law Enforcement Agency's project manager will grant access to the Federal Law Enforcement Agency personnel involved as volunteers in testing based on testing location and staffing constraints.

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 tests include personnel operating a single remote server which will centralize the receipt and dissemination of test images. Images related to the test periods are routed to a specific server and are accessible only to the industry performer's project manager and IT manager. These images will only be retained for 24 hours.

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.

The risk associated with the RealEyes research is that unauthorized personnel would gain access to the images collected during the experiment. To mitigate this risk, S&T will instruct all participants to make every effort to avoid capturing images of passers-by. Further, no images will be stored on the PDAs used during the testing so testers will not have access to the images other than the live streaming video. Additionally, images will only be stored for a maximum of 24 hours on the industry performer's server.

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)
- ☐ Federal government agencies (please specify)
- ☐ Private entities:
  - ☐ Businesses in monitored areas
  - ☐ Insurance companies
  - ☐ News outlets

☒ **Other (please specify)**
The industry performer will oversee the testing events and will have access to the images for the length of the 24-hour retention period. The industry performer's project manager and IT manager will be responsible for destroying the images and no one will have authority to alter or enhance the images while they are retained on the server. When the industry performer deletes the images, they will send the Federal Law Enforcement Agency and S&T project managers confirming the deletion of all images utilized during the testing period.

☐ 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 industry performer will have access to all utilized images during the testing period because they have developed the technology that is being tested to determine if any changes or improvements are necessary to meet the needs of the Federal Law Enforcement Agency. The industry performer must have complete access in order to run the test and gauge the performance against the Federal Law Enforcement Agency's requirements.
Rules & Regulations: The industry performer may only retain the images for 24 hours and must delete them at the end of the 24-hour retention period.
Disclosure: S&T will not share the images with the industry performer for any purpose other than continuing development of the technology.
Authority: S&T is sharing the information pursuant to Subchapter 3 §182 of the Homeland Security Act, which assigns the Under Secretary for Science and Technology the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities.

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**

Industry performer representatives will have access to images during the testing period via PDAs and to the stored images on the server. The industry performer's project manager and IT manager will be responsible for deleting the images from the server. No images will be enhanced or altered during the 24 hour period; the window is to address post-testing follow-up questions or issues from the Federal Law Enforcement Agency regarding the technology's capabilities only. The industry performer has recently upgraded the encryption to their system and all video utilized during the testing period will be transmitted to, from, and between the PDAs using SSL 128-bit encryption.

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**

S&T has a test-bed and services contract with the industry performer. The RealEyes technology is already commercially available; therefore the contract with the industry performer provides specific support to the Federal Law Enforcement Agency's demos and scenario testing.

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)
☐ 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 industry performer will have access to the live, streaming video images and the recorded images. To enhance the security of these images, they will not be stored on the PDAs used during the research. Images utilized during the test phase will only be retained for 24 hours on a server belonging to the industry performer. Only the industry performer's project and IT managers will have access to the stored images and will be responsible for deleting the images after 24 hours.

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 PDAs utilized and the captured images will be retained on an industry performer's server for a maximum period of 24 hours. The industry performer's latest system software upgrade implemented 128-bit encryption. All video utilized during the testing period will be transmitted to, from, and between the PDAs using this SSL 128-bit encryption.

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 testing period. The industry performer's project manager and IT Manager will have the sole access to the stored images and will delete the images after 24 hours. At the end of the 24 hour period, the industry performer will send an email to the Federal Law Enforcement Agency and S&T project managers confirming deletion of all images utilized during the testing period.

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**

All Federal Law Enforcement Agency test subjects, S&T project management team members, and industry performer representatives will have access to real-time images of the images on the PDAs.

☐ 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)**

Only the industry performer's project manager and IT manager will have access to the stored images. The images will be deleted after 24 hours.

☐ 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)**

When they arrive at the testing location, the volunteers from the Federal Law Enforcement Agency will be given a document making them aware that the industry performer will be retaining all testing images on a remote server for a period of 24 hours after which they will be deleted. Additionally, the document will instruct all participants to make every effort to avoid capturing any images of persons not involved in the testing.

☐ No

6.1.3 When access is granted:

☒ There are ways to limit access to the relevant records or technology (please specify)

No images will be maintained on the PDAs utilized during the testing period and test participants will not have access to any captured images following the conclusion of the testing event. The industry performer's project manager and IT manager will have access to the captured images and will be responsible for deleting all images after 24 hours.

☐ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

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

There is no current procedure for auditing because the images will be deleted after 24 hours. All research participants will have access to the images, via the utilized PDAs, during the testing period. No images will be maintained on the PDAs following the conclusion of the testing period. Only two people will have access to the images while they are stored on the remote server: the industry performer's project and IT managers.

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)-**

Verbal instructions issued by the DHS S&T Project Manager.

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

There is no current procedure for auditing because the images will be deleted after 24 hours.

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 individual may gain access to the images. In order to mitigate this risk, the PDAs utilized by the research participants will not store any information and all images associated with the testing will only be retained on a server belonging to the industry performer for 24 hours following the conclusion of the testing. The industry performer's latest system software upgrade implemented 128-bit encryption.

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**
☒ **Other (please describe)**

S&T will provide explicit notice to all volunteers from the Federal Law Enforcement Agency participating in the project that their images will be collected and the purpose for collection. Any streaming or capture of images beyond those of the Federal volunteers will be inadvertent and avoided to the greatest extent possible. No images will be stored on the PDAs or retained longer than 24 hours. In order to effectively gauge the operational efficiency of the RealEyes system for the Federal Law Enforcement Agency's use, the testing conditions must simulate those encountered in the field as closely as possible. This would include crowd situations where the public is unaware of ongoing Federal Law Enforcement Agency operations. Because of the necessity to replicate operational situations and given that all utilized images (including those of inadvertent passersby) will be purged within 24 hours.

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 testing is to research and actualize the needs of the Federal Law Enforcement Agency for the possible future application of this technology. Any use of

privacy enhancing technology, in this initial stage of research and development, would dilute the effectiveness of the test results.

Responsible Officials

John Price

Science and Technology Directorate

Department of Homeland Security

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.