Privacy Impact Assessment
for the

DHS Sensor Web

January 20, 2010

Contact Point
Dr. Kai-Dee Chu
Command, Control, and Interoperability Division
Science and Technology Directorate
202-282-8000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Abstract

The Sensor Web project is a research and development effort funded by DHS Science and Technology Directorate (S&T) Office of Small Business Innovation Research (SBIR) that seeks to develop and test the effectiveness of a smart sensor system for potential law enforcement and first responder applications. The technologies being tested—video recording technology and analytic tools to interpret and process that video—are technologies that potentially impact the privacy of individuals, both during the tests and in future live settings. This PIA contemplates the immediate privacy impacts of conducting the tests as well as the more general privacy impacts of the technology itself.

Overview

DHS S&T SBIR Office is funding two research performers through a contract to conduct research, development, testing and evaluation activities on their respective Sensor Web systems. The Sensor Web project will develop and test an end-to-end smart sensor system prototype to test integrating data from video imaging inputs into a network and distinguishing target items from the rest of the video imaging inputs for law enforcement or first responder applications. This technology is being tested because image capture may be applicable to a variety of law enforcement applications such as anomaly detection (e.g.; a left bag or target intrusion). The technologies tested—video recording technology and analytic tools to interpret and process that video—are technologies that potentially impact the privacy of individuals, both during the tests and in future live settings. This PIA contemplates the immediate privacy impacts of conducting the tests as well as the more general privacy impacts of the technology itself.

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." To meet this statutory mandate, S&T must explore a wide variety of cutting-edge technologies, many of which impact privacy due to the very nature of the technology itself. In conducting this PIA, therefore, S&T is not conducting an analysis of the privacy risks undertaken to meet its legislated mandate. Rather, this PIA is intended to address the privacy impacts of conducting the Sensor Web test given that a test of this type is authorized and necessary.

Previous Development: Phase I and Preparation for Phase II

This project is structured into two phases. Phase I, which has concluded, consisted of the design and refining of the Sensor Web system hardware, software, and algorithms; primarily the back end of the system. Phase I only focused on the development of the Sensor Web technology; it did not involve the collection of any personally identifiable information (PII). As Phase I has concluded, S&T has selected two research performers and funded contracts with them to perform Phase II testing. The objective of Phase II testing is to evaluate the effectiveness of each performer's respective Sensor Web system in integrating input from the video imaging sensors into a network and distinguishing targets or items of interest from unimportant data in a captured frame.

Prior to operational testing, the performers will have conducted extensive laboratory testing of the developed video sensor system. During the testing, the network (to include the sensor systems, server, and back-end system) will employ encryption technologies to protect the wireless transmission of video images.

The project will involve the following participants:

1. S&T, who will provide funding to the performers for the development and testing of the sensor system. S&T will provide technical and programmatic oversight during the testing, but will not have access to or retain any images collected or generated during the field tests. S&T will only receive final reports documenting the effectiveness and evaluations of the systems while observing demos of the Sensor Web technology.
2. The contracted Phase I/Phase II performers, who will develop the Sensor Web system and conduct tests in an operational setting using volunteer research participants from their internal testing and evaluation team. The performers will also provide onsite technical and logistical support.

Current Development: Phase II

The two Phase II performers will conduct the testing activities in an operational setting using internal employees (members of the performer testing and evaluation team) as research volunteers. It is anticipated that testing will occur within the performers' offices, at airports, and possibly border crossings. Testing activities will involve capturing live streaming video and images of research volunteers using the imaging sensors. The research will focus on the height or outline of a person (performers will develop video imaging sensors to distinguish between persons and vehicles), distinguishing characteristic of an item of clothing (such as the color or specific pattern of a shirt), or items deliberately placed by research volunteers. The sensors will capture video data and push everything to a dedicated server where the majority of the analysis will occur. Any anomalies (such as left bags or attempted unauthorized access by volunteers) will be indentified by the server system algorithms and will be pushed to the user interface as a warning to bring user attention to the possible issue. The user will not receive all captured information, just that which has been identified by the server system algorithm as an anomaly. Performers will delete all data collected within 24 hours after the conclusion of each testing period. Both of the performers will follow a similar project plan in order to deliver the end-state technology or deliverables requested by DHS S&T and S&T customers; however each will have unique project aspects and utilize internal development capabilities to reach the overall project goal.

By testing the effectiveness of the developed system, performers can determine the utility of the technology to first responders and law enforcement officers in real-world situations, such as locating occupants in a burning building. The intended benefits of a Sensor Web system will be providing the potential law enforcement and first responder users with technological capabilities to better process video imaging input to detect targeted items/intruders, enable more access to a multitude of information during emergency situations, and increase situational awareness – all of which are critical for the law enforcement and first responder community, especially when situations require quick decision-making.

Post-Transition of Technology to End User

Ultimately, S&T envisions the system integrating multiple sensor inputs (e.g., chemical, biological, nuclear, environmental) into the network to form a sensor web for the system to process data individually and collectively, which will provide a wealth of knowledge critical for situational awareness for first responders or other end users. The type of sensors integrated into the system is dependent on the needs of the end user and inclusion of any such sensors beyond the video capture sensors tested during Phase II of this project would occur after transition. For example, some end users may only integrate the video imaging sensors into the system, while others may integrate chemical and biological sensors into the system. S&T would update this PIA prior to the inclusion of any additional types of sensors into the test or live environments.

This PIA covers only S&T's research and development process for the Sensor Web system. Should the S&T customer acquire the technology being tested, the customers would be responsible for conducting a separate PIA to cover operational uses.

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

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed.

1.1 What information is to be collected?

(Please check the following if applicable)

The System's Technology Enables It to Record:

☒ Video

Static Range: 60-65 ft or 16-bit

Zoom Range: 35-40 ft or 1-5x

☒ 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 research volunteer images via image sensors deployed to simulate real world applications. Performers will make every effort to confine the captured images to volunteers from their internal testing and evaluation team. However, it is possible that incidental images of passersby could be inadvertently captured in the background of the images of volunteers during the testing.

Performers will not use any incidental images captured during testing activities as part of testing data. One performer's envisioned system has the capability to "wipe out" unimportant background images, and focus on a specific target item. While the performer will begin the development of the "wipe out" capability in Phase I, the performer will conduct the tests of this capability in Phase II. The performer will aim to include the "wipe out" capability into the technology by the conclusion of Phase II. The other performer has not yet indicated that its system will contain this “wipe out” capability.

In most cases, the performer will only see the cleaned images containing only the images of items of interest during the tests. Additionally, the user will never have complete access to unfiltered streaming images. The images sent to the user will instead be defined by the server system as those that require user attention (such as unauthorized access or an unattended object). DHS S&T will not have access to or retain any images, whether of volunteers or unintended bystanders, during or following the conclusion of the testing period.

□ 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.

One or more screenshots of a typical recording may be a helpful item to include in an appendix.

1.2 From whom is the information collected?

□ General public in the monitored areas.

☒ Targeted populations, areas, or activities (please describe).

Performers will capture images of volunteers participating in the testing activities. However, performers may inadvertently capture incidental images of passersby in the background.

☒ Training included directives for program officials to focus on particular people, activities, or places (please describe). Performers will be instructed to take all possible measures to minimize image capture of individuals not involved in the project. Performers will make every effort to confine the captured images to volunteers from their internal testing and evaluation team. This includes making every effort to only capture images only of research volunteers working directly on the testing activities.

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

Under the instructions of program officials, performers in this project will attempt to capture only images of research volunteers and make every effort to avoid capturing images of passersby.

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 conduct testing and evaluation activities on the Sensor Web system to determine its effectiveness in integrating data from video imaging inputs into a network and distinguishing target items from the rest of the video imaging inputs for law enforcement or first responder applications. This type of image capture is applicable to a variety of law enforcement applications such as anomaly detection (e.g. – a left bag or target intrusion). During the Phase II testing period, the focus will be on anomaly detection through video sensors. To test this capability, members of the research team will volunteer to stage scenarios (in front of the video imaging sensors) to determine how effectively it can detect or identify anomalies. For example, research volunteers may deliberately leave behind a bag to determine whether the system will identify it as an anomalous item to the performers at the user interface. During these tests, the performers will strive to only capture images of the volunteers and items that volunteers may incorporate into the test activities (i.e., bags).

Integration of other sensors will be undertaken by future customers after transition. Performers will store all images captured during the testing activities on their own respective, dedicated servers, and for the purposes of the testing period, performers will delete all information on their servers within 24 hours following the conclusion of each testing period.

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, develop, demonstration, testing, and evaluation activities to support all elements of DHS. The Sensor Web project is a research, development, testing and evaluation effort to support DHS's mission of keeping terrorists and their weapons out of the U.S. and securing and facilitating trade and travel. The tests will aid DHS component customers, law enforcement, and first responders in determining whether to acquire the system and how best to utilize the system. The greatest benefit of the system is the ability to integrate information from multiple sensors in various locations into one sensor web and distinguish target items in a captured to provide users with better detection capabilities, increased situational awareness, and greater access to information during emergency situations. Additionally, the system reduces the burden of surveillance on the part of the end-user by targeting anomalies to direct user attention.

☐ 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 footage is 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 intended benefits of the overall Sensor Web system will be providing the potential users with technological capabilities to better analyze video imaging sensor input to detect targeted items/intruders and increase situational awareness – both of which are critical for the law enforcement and first responder community, especially when situations require quick decision-making.

The placement of the video imaging sensors is only for research and development purposes. Researchers will place the video imaging sensors in isolated areas to minimize the incidental image capture of passersby not involved in the project. The eventual end user of the system will determine the operational placement of the video imaging sensors, which will depend on their needs and use of the system.

The capability for robust data integration from video imaging sensors and target recognition may enhance the situational awareness of S&T customers, law enforcement agents and first responders in the field, allowing them to better prepare for emergency situations. By integrating data from the video imaging sensors, the system will be able to develop a comprehensive understanding of an emergency environment and allow law enforcement and first responders to safely perform their duties. During the Phase II tests, the two performers will conduct testing activities on the anomaly detection through video sensors in an operational test setting using internal employees (members of the performer testing and evaluation team) as research volunteers. It is anticipated that testing will occur within the performers' offices, at airports, and possible border crossings. Researchers will deliberately place the sensor systems in isolated areas, where there are fewer passersby, so that they can focus on the research volunteer activities. During the tests, researchers may deliberately place a bag within the view of the video imaging sensor and will determine whether the system can effectively identify the bag as an anomalous object. Other similar tests may be conducted during the project. Performers will also test how effectively the system can determine objects, specifically, distinguish a human from a vehicle. To test this capability, images of the research volunteers may be captured during the testing activities.

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 footage is collected to compare to terrorist watch lists and wanted persons lists.

The Sensor Web system will supplement the work already being done by DHS customer components, law enforcement, and first responders to accomplish their individual missions. Ultimately, the Sensor Web system being developed will increase the situational awareness capabilities of such agencies. The videos will only be utilized during the course of the testing period and performers will delete all information from the server within 24 hours following the conclusion of each testing period.

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 performers will evaluate the Sensor Web system by determining the accuracy in which the system’s algorithms can distinguish target items from the rest of the video images captured. For example, performers will analyze how effectively the system can distinguish a person from a vehicle, or how effectively the system can detect and target a bag, deliberately placed by a research volunteer. The performers will also evaluate how efficiently the system analyzes the input by assuring that the information reaching the user interface is identical to the information requested of the sensors. Using these test results, the performers will compile a final report documenting the results and analyzing its utility for real life application. S&T and S&T customers will receive the final reports.

Situational awareness is essential to the operational missions of DHS components, law enforcement, and first responders. These agencies continue to search for more efficient methods to increase surveillance capabilities. The Sensor Web system, if deployed, will greatly increase the situational awareness capabilities of these agencies. When in use, the system will decrease the burden of surveillance by being appropriate for use in unmanned areas and sending automatic information to end users to follow-up on anomalies captured though the sensors – limiting the time necessary to monitor video feeds.

1.3.2 Cost Comparison

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

Although there are a number of private companies currently developing sensor technologies, those products have not been developed and tailored to the specific mission needs of DHS component customers, law enforcement and first responders. Additionally, the technologies funded through this effort are more cost-efficient because network infrastructure already exists. Because of the use of the SBIR program, the development for Phases I&II is more cost effective than other private development programs. While the sensors play a major role in the project, the sensor web capability is equally critical for the success of the system. Through the SBIR program, S&T is funding the development of both the video imaging sensors, and the accompanying sensor web systems, rather than developing, acquiring, and/or integrating the two capabilities separately. S&T market research found that current commercial off the shelf (COTS) sensor systems do not cover all the state-of-the-art technologies and network infrastructure that these Sensor Web projects will develop. The effort focuses on the development of a wireless, self-forming sensor network, rather than on the sensors themselves. The self-forming networks would provide a more infallible system, which means in the event that one of the sensors dies or goes off line, the rest of the sensor web network will "reform" without a gap. Additionally, some COTS systems still use proprietary technologies that are difficult to integrate.

1.3.3 Effectiveness

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

Performers will compile a final report at the conclusion of the testing activities documenting test results and analysis of the system's effectiveness. S&T and the potential DHS component customer will receive and review this final report, and provide a qualitative evaluation of Sensor Web 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 footage streamed, but not stored.

☒ Real-time monitoring with footage stored.

Each performer will store images on a dedicated server, but all information will be deleted within 24 hours following the conclusion of each testing period. It is anticipated that each testing period will last for one or two day periods. It is not expected that any one test will be longer than two days.

☐ Footage 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?

Performers will delete any images captured during Sensor Web testing within 24 hours of the conclusion of the test. All images collected from the sensors will be sent to the dedicated network server which will be purged following each test for the length of the project. Only the performer's IT manager working directly on the project will have access to any information collected and sent to the server.

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 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.

☐ 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)

Each of the two Phase II follow-on contracts will have an 18 to 24 month period of performance. Phase I, which did not require the use of PII, was already funded and has concluded.

☐ 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 minimize capturing images of individuals not involved in the project. This will include posting signs to notify passersby that sensor tests are ongoing to minimize entrance into testing areas. Efforts will first be made to conduct testing in areas that are less likely to have passersby. If the testing is conducted in public venues, there will be signs notifying the public that testing is occurring and to avoid the area. Additionally, performers will delete any images collected by the sensor network during testing within 24 hours of the conclusion of each testing period.

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 privacy risk associated with the Sensor Web research project is that performer could inadvertently capture images of passersby without the knowledge or consent of those individuals, or deliberately capture images of the public during the tests. To mitigate this risk, performers will make every effort to avoid capturing images of passersby and confine the captured images to volunteers from their internal testing and evaluation team. Performers will also post signs to notify passersby that sensor tests are ongoing to minimize entrance into testing areas. All efforts will first be made to conduct testing in areas that are less likely to have passersby. If the testing is conducted in public venues, there will be signs notifying the public that testing is occurring and giving the public the prerogative to avoid the area if they do not wish to be recorded. The sign will read: "Homeland Security surveillance technology testing in progress. Please avoid this area. Images may be captured upon entering this area."

An additional privacy risk is unauthorized access to the information collected during the tests. To mitigate this risk, performers will employ encryption technologies to protect the network which images are transmitted. Performers will limit access to the network using password protections in which only performers working on the project will access to the network.

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 footage. 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.

During the S&T-funded testing period, the images captured by the Sensor Web will only be used to test the strength and operational capabilities of the two Sensor Web systems.

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 project will be instructed to minimize the image capture of individuals who are not associated with testing. The information will be stored on the performer's dedicated server for 24 hours for post-testing period evaluation, after which time they will be destroyed. Additionally, the Sensor Web system will only push relevant information (images of target items) to the users. The user will not receive all captured information, just that which has been identified by the server technology as an anomaly. For this project, an anomaly is clearly defined (e.g., a bag left sitting for a long period of time or a person walking against the flow of traffic) and will be determined by the performers. In theory, if a person enters the surveillance area during the testing period and was behaving strangely for an extended period of time, they might show up as an anomaly; however it does not seem likely.

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 data in the system (i.e., how long is footage 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

Performers will retain the images captured during the testing for a maximum of 24 hours on the dedicated Sensor Web system belonging to each of the performers utilized during the test period. The performers require this short retention period to revisit the testing conditions if any immediate questions about the technology’s abilities should arise during and after the test.

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

☐ Footage automatically deleted after the retention period expires

☒ System operator required to initiate deletion- Each performer will delete all images collected within 24 hours following the conclusion of the testing period. The performer will send the S&T program manager an email confirming that all collected images have been deleted. The program manager will have close contact with each performer during the whole project. The program manager will work with the performers to develop and approve the testing scenarios.

☐ Under certain circumstances, officials may override detention period:
- ☐ To delete the footage before the detention period
- ☐ To retain the footage 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 performers will retain any information collected from the sensors, including images, on the Sensor Web server for a maximum period of 24 hours, after which time the images will be destroyed. This time period allows the performers 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 –S&T will not have access to or receive any images, therefore will not share any information with internal entities. Furthermore, only performers on the testing and evaluation teams will have access to the images; the performers will not share the information with any internal organizations.

Classes of Personnel

□ Command staff (please specify which positions)
□ Middle management (please specify)
□ Entry-level employees
☒ Other (please specify): Only performers on the testing and evaluation team will have access to the images; the performers will not share the information with any internal organizations. Members of the performer teams will include IT managers, system engineers, and project managers.

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)?

The performers will not share images captured with any internal DHS entities, including S&T. Only members internal to the performer research team will have access to the images captured during the tests. S&T will not have access to or receive any information collected during the testing period, therefore will not share any information with any internal entities.

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

☐ Yes (please detail)
☒ No S&T will not have access to or receive any information.

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

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) S&T will not access or receive any information, therefore will not share any information.

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.

S&T will not have access to or receive any images captured during the testing activities. Neither S&T nor the performers will share the information with any internal entities. The performers will delete all images collected within 24 hours following the conclusion of the testing period. The performer will send the S&T program manager an email confirming that all collected images have been deleted.

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

Performers will oversee the testing activities and will have access to the images collected from the Sensor Web for the duration of the testing period.

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 footage

Purpose: The performer will have access to all collected 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 DHS customer. The performer must have complete access in order to run the test and gauge the performance against the user requirements. The performers will not share images with any individuals or agencies outside the performer testing and evaluation teams.

Rules & Regulations: The performer may only retain the images for 24 hours and must delete them at the end of the 24-hour retention period.

Disclosure: No images will be shared with any parties aside from the performers under contract for this work.

Authority: S&T is sharing the information pursuant to Subchapter 3 §182 of the Homeland Security Act, which assigns the Undersecretary 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 footage shared on a case-by-case basis
□ Certain external entities have direct access to surveillance footage
□ Real-time feeds of footage between agencies or departments
☒ Footage transmitted wirelessly or downloaded from a server
□ Footage transmitted via hard copy
□ Footage may only be accessed on-site

The video imaging sensors will collect information, including images, during the testing period. These images will be transmitted wirelessly to the dedicated server. Performers will perform all wireless transmissions over encrypted networks to ensure the security of the images. The performer representatives involved in the testing will have access to images on the server and those that are transmitted as warnings to the user console. No images will be stored on the user console during testing and all images will be deleted from the server within 24 hours of the testing period. The images will not be shared with any individuals or agencies outside the performer testing and evaluation teams. The images will not be shared with any individuals or agencies outside the performer testing and evaluation teams.

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

The images will not be shared with any individuals or agencies outside the performer testing and evaluation teams.

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 performer's internal IT director will be solely responsible for ensuring that all information collected during the testing period is removed from the server within 24 hours. The images will not be shared with any individuals or agencies outside the performers testing and evaluation teams.

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, performers will not share images with any individuals outside the performer's testing and evaluation team. Performers will also employ encryption technology to protect images stored on the network. All networks will be password protected to limit access to only authorized users.

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 during the testing period – the project will test the sensor network structure and the effectiveness of the user interface. The performer's IT director will be the sole person responsible for deleting all information collected from the servers during the testing period. This will occur within 24 hours following the conclusion of the each 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 footage

☒ Only certain authorized users have access to real-time footage (please specify which users)

The performer team will have access to real-time footage during the testing period. Following the conclusion of the testing, only the IT manager will have access to the information residing on the server. The IT manager will be responsible for deleting all information collected during the testing from the server at the end of the 24 hour period. The S&T project manager and the potential DHS component customer representative may be present for some part of the testing – solely as observers with no direct access to images.

☐ All authorized users have access to stored data

☒ Only certain users have access to stored data (please specify which users)

The performer's internal IT director will be the only participant to have access to the images collected from the sensors and sent to the dedicated server following the testing period. The IT director will be responsible for deleting all information from the server within 24 hours following the conclusion of the testing period.

☐ 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 footage

☒ Only certain authorized users can delete or modify footage (please specify which users)

No images will be modified. The performer's IT director will be responsible for deleting all images collected during the testing period within 24 hours.

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

☐ Yes (please specify)

☒ No

User access to the system will be limited to the performer's internal staff. All members of the performer team will be advised that all efforts should be made not to capture images of bystanders. There will be no additional users involved in the testing of the Sensor Web system.

6.1.3 When access is granted:

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

The user console will not retain any information, and the performer will delete all information collected from the network within 24 hours following the conclusion of the testing period.

☐ 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 currently no method for auditing who accesses records or track uses because the performers will delete all images collected within 24 hours following the conclusion of the testing period. At the end of the 24 hour period, the performer will send the S&T program manager an email confirming that all collected images have been deleted.

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)

S&T will provide web-based privacy awareness training to all performers involved in the project. The training will provide guidance to performers on how to properly safeguard, store, and handle PII. Additionally, all performer testing and evaluation teams will be trained on how to properly use the system, and instructed to make every effort to only capture the images of volunteer participants.

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 currently no system for auditing because performers will delete all collected images within 24 hours following the conclusion of each testing period. The performers will send the S&T program manager an email confirming that all collected images have been deleted.

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)

There is currently no system for auditing because performers will delete all collected images within 24 hours following the conclusion of each testing period. The performers will send S&T program managers an email confirming that all collected images have been deleted.

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 unauthorized individuals may gain access to the images. In order to mitigate this risk, performers will make every effort not to capture images of individuals who are not associated with the testing activities. Performers will also employ encryption technologies to protect the wireless transmission of images and password protect the network so only authorized performers will have access to the images.

Another privacy risk is noncompliance due to the fact that there are no auditing mechanisms in place. To mitigate this risk, S&T provides privacy awareness training to all contracted research performers to ensure that they are aware of their responsibilities in handling and protecting PII. Additionally, the performers will send S&T program managers email confirmations once all images collected are deleted.

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: "Homeland Security surveillance technology testing in progress. Please avoid this area. Images may be captured upon entering this area".

□ Notice is not provided

□ 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

Prior to Phase II testing, Phase I of this project will have evaluated a number of technologies through proposals. The two performers funded for the Phase II period were determined to have technologies comparable, or exceeding, the technologies also available on the market.

8.2 What design choices were made to enhance privacy?

□ The system includes face-blurring technology

☒ The system includes blocking technology. This technology will be developed and eventually tested by one of the two performers before the end of phase II.

□ The system has other privacy-enhancing technology (Please specify)

□ None (Please specify)

A capability is being developed that will allow the Sensor Web system to capture an image (streaming video) and identify an object (specifically a bag being left behind) that is not moving but has been added to the captured area. The dedicated server will have the capability to single out the stationary object of interest and wipe the rest of the image (of crowd, furniture, etc). This process will be done before the images reach the back-end user-driven part of the system. The original images may be sent to the dedicated server, but following the conclusion of the testing the images will be deleted from the server.

Responsible Officials

Dr. Kai Dee Chu

Department of Homeland Security

Approval Signature Page

Original signed and on file with the Privacy Office.

____

Mary Ellen Callahan

Chief Privacy Officer
Department of Homeland Security