Privacy Impact Assessment
for the

Critical Infrastructure Change Detection

September 4, 2009

Contact Point
John M. Fortune
Infrastructure/Geophysical Division
DHS Science and Technology
(202) 254-6622

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Critical Infrastructure Change Detection (CICD) program (also known as the Wide Area Surveillance program) is a DHS Science and Technology (S&T) research program that is examining novel technical approaches to provide wide area surveillance and change detection capabilities to protect the Nation's critical infrastructure. S&T proposes to test a high resolution, 360 degree field-of-view video system that will accommodate multiple simultaneous users and also have change detection and tracking capabilities. A PIA is being conducted because system demonstrations will be performed in public areas within major US cities and will involve capturing images of persons and textual information in the public space.

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."

CICD is an S&T research program that is examining novel technical approaches to provide wide area surveillance and change detection capabilities to protect the Nation's critical infrastructure. The project is part of the S&T Innovation portfolio, which aims to provide proof of concept for new technology solutions. S&T is charged with developing technology solutions to protect critical infrastructure, as defined in Homeland Security Presidential Directive-7 and the National Infrastructure Protection Plan.

One of the big challenges for surveillance of urban infrastructure is obtaining total situational awareness of the surrounding area. A threat may involve people casing a facility, carrying unusual items, etc. The goal of CICD is to develop a system with the optical resolution and analytic capabilities to facilitate better detection of such threats. For this program, algorithms are not being tested to identify specific individuals.

Effective wide area surveillance requires total situational awareness of potential threats in the vicinity of urban assets. Threats could be posed by an individual, object, or vehicle. The CICD system under development for this project will provide high resolution real-time and forensic surveillance of urban infrastructure and the surrounding area (to include vehicular and pedestrian traffic). The CICD system is designed to provide high resolution imagery and allow tracking of people and vehicles throughout a complex urban scene. It will allow multiple operators to simultaneously view and manipulate (e.g., zoom, scan) regions of the scene in high resolution detail while maintaining a full 360 degree field of view. The system includes automated change detection capabilities, and users will be able to rapidly scan video images for forensic analysis. This project is divided into multiple phases with milestones for demonstrating several prototype versions of the system, each phase representing significant advances in wide area surveillance technology.

The first phase will employ an array of multiple high resolution cameras that are digitally integrated into a single view with an overall field of view resolution of 100 Megapixels. A second phase under development will utilize a single multi-lens imager based on military technology that will provide even greater resolution.

Pacific Northwest National Laboratory and MIT Lincoln Laboratory (referred to hereafter as "the Labs"), which are under contract with S&T for the CICD task, are designing and developing the system. S&T has developed partnerships with Federal, State, and local agencies as potential users for the CICD project technologies.

Demonstrations are not intended to be law enforcement exercises. Participating agencies will be present to evaluate the utility of the technology and provide feedback to DHS, but will not be making operational or law enforcement decisions as part of the demonstration. These agencies will provide user requirements for the system and will evaluate system effectiveness during the project demonstrations.

Demonstrations will occur in areas recommended by the agencies, and preferably where cameras are already operating. System will be temporarily installed and operated for a minimum of one week. Personnel from the Labs will bring the system to the designated site, provide onsite management of the system for duration of the demonstration, and remove the equipment at its conclusion.

The CICD test system will collect images to test the system's effectiveness (e.g., effectiveness of digital image stitching, multiple operator use, resolution and zoom, ability to track cued images, change detection in exclusion zones, and semi-automated forensic analysis). The CICD system will be operated by personnel from the Labs, S&T, and the participating agency. The computers, operator stations, and the optical sensor will be configured at MIT Lincoln Laboratory, brought to the demonstration site and positioned in such a way to optimally collect images without significantly impeding pedestrian traffic. Signs will be posted in several locations throughout the area to notify the individuals of the ongoing surveillance activities. The specific configurations for mounting of the optical sensor (i.e., the camera) and installation of user workstations will be based on logistics of the demonstration site. For example, in outdoor laboratory testing of the CICD system, the optical sensor was mounted on a mast attached to a trailer, and monitors were installed in the trailer to allow multiple users to simultaneously operate the system.

Lab personnel will be the primary operators, as they best understand system operation. S&T and agency partners will operate the system for the purpose of evaluating its effectiveness and providing feedback to the Labs to help guide future system development. The agencies will not make any operational or law enforcement decisions and will not engage in any routine law enforcement actions based on the CICD test system. The CICD system and the images collected during the test will only be used for research and development purposes. However, in the event that a law enforcement investigation occurs due to an incident within the area monitored by the CICD system, the footage related to that specific incident could potentially be utilized during the course of an investigation.

Following the demonstration, Lab personnel will remove the CICD system from the demonstration site and collect technical evaluation data from the participating agency and the S&T program manager. The effectiveness of the systems in the demonstrations will guide further development and addition of capabilities.

The following questions are part of the CCTV PIA template and 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: To be determined
  - Zoom Range: To be determined
- ☒ 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.
- ☒ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
  One of the project goals is to effectively track images, which could include persons, vehicles, or other objects (all of which could pose a threat to urban infrastructure). Since the system includes a high resolution optical sensor that captures full 360 degree imagery, it will automatically capture images of any persons, text, or other object within range of the CICD system. Having the capability to collect and process high resolution images of persons, vehicles, license plates, unusual objects, etc is a critical component of developing effective wide area surveillance technologies to protect urban assets. All images within the coverage area (persons, vehicles, and anything else) will automatically be captured. No one will be targeted, but these images will be used to test the functionality of the system. Images of individuals will only be used to test the resolution of the cameras and the ability to track a person moving in a crowded urban environment, not to determine the identity of the individual.
- ☐ 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 - movement into access-controlled areas.
☐ 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.

An important component of the CICD system is the ability to detect changes against a normal background. One way the demonstration will test change detection will be the ability of the system to detect movement of pedestrians and vehicles into and out of access-controlled areas. Change detection algorithms are being developed that will attempt to detect objects that have entered the targeted area. The CICD system may also capture images of people as part of the demonstration and system evaluations, but specific populations will not be targeted.

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) – Research purposes, to test system functionality

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 CICD research is testing a technology that would provide wide area surveillance and change detection capabilities to protect the Nation's critical infrastructure.

☐ 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 CICD system is designed to provide high resolution full-scene recognition and change detection in complex urban environments to protect critical infrastructure assets contained within such areas. The system has already undergone extensive laboratory testing, and now needs to be tested in a real-world urban setting. The laboratory testing has been performed in a campus parking lot with minimal traffic (both pedestrian and vehicular). This preliminary phase of testing was necessary to work out the glitches in the system, allow improvements to be made in the system, test specific capabilities (such as internal camera-to-camera handoff), and achieve a sufficient level of performance prior to testing in a real world environment. The campus parking lot was chosen because of its close physical proximity to the laboratory and because it is located in a secured facility, where only authorized personnel and laboratory employees are allowed, thus minimizing risks to the public. In the preliminary tests, the CICD system was temporarily mounted to collect data and a trailer was used to store computer servers and work stations. The intent of the real-world test in a crowded urban environment is to stress the system to see if the same functionality can be achieved. The complexities presented by a congested, rapidly changing urban landscape cannot be fully simulated in a laboratory. For example, continuous tracking of an individual or vehicle throughout a complex scene (with many other individuals, vehicles, and objects), to include passing from one camera to the next within the system, is a capability that is yet to be tested. It is also critical at this point in the project for an end-user to evaluate the technical capabilities of the system in a real-world environment and provide feedback to S&T in order to inform future research and development.

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.

S&T and the Labs are collecting the images for research purposes in order to develop a system that can provide high resolution full-scene recognition and change detection in complex urban environments to protect key infrastructure assets. Effective surveillance of urban infrastructure requires persistent imaging and total situational awareness of the surrounding area, such that threats in the form of persons, vehicles, or objects can be readily identified. The CICD system is being developed to provide 360 degree full-scene imagery with much higher resolution than is currently available, and to enable the system hardware for tracking of people and vehicles throughout a complex urban scene.

The CICD system and the images collected during the test will only be used for research and development purposes. However, in the event that a law enforcement investigation occurs due to an incident within the area monitored by the CICD system, the footage related to that specific incident could potentially be utilized during the course of the investigation.

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 evaluation metrics are related to the technical capabilities of the system. Sample questions include: Is digital image stitching effective for complex scenes? Is the resolution acceptable? Can tagged persons, vehicles, and objects be effectively tracked within a complex environment? Are certain changes (e.g., vehicle in an exclusion zone) detectable in a cluttered urban background?

1.3.2 Cost Comparison

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

The purpose of the CICD program is to develop innovative technologies to protect the Nation's critical infrastructure through wide area surveillance and change detection. This includes proof of concept technology demonstrations. S&T has considered multiple technologies and platforms for wide area surveillance and change detection. S&T is pursuing the technology being tested because its capabilities are significantly greater than any commercially available technologies. There is no other technology against which to measure cost effectiveness.

1.3.3 Effectiveness

- ☒ Program includes evaluation of systems performance (please describe how performance is evaluated.) See 1.3.1.3 above.
- ☐ 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.
- ☐ 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?

As a matter of program policy, S&T and its contracted Labs (and their subcontracted vendor partners) will not alter or enhance the images either before or after storage. The raw video images will only be used for research and development activities. Only authorized individuals associated with the project will have access to the stored images. The video images will not be altered or enhanced either before or after storage. Once the project concludes, all video images will be destroyed. Authorized individuals will be employees of the DHS, the Labs, and/or subcontracted vendor partners and have a legitimate need to access the images. The Project Manager will grant access to the images only after an authorized individual demonstrates a legitimate need. The Labs will store the images. Images may be transmitted to subcontracted vendor partners for use in algorithm development, and returned to the Labs for storage when no longer being actively used. While the images are not being actively used, the Labs (and their subcontracted vendors) will treat the images as sensitive information and protect it accordingly. This includes storing the archived images in a locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images. Although no system-specific auditing mechanisms are planned, the Labs (and their subcontracted vendors) have IT security measures in place to ensure that the systems on which the images are stored are only accessed by authorized personnel. Each of the authorized individuals accessing the images will undergo training and/or briefings detailing DHS privacy policies and the protection of information including sensitive personal and for official use only.

Individuals attending the demonstration will have the ability to view the images during collection, but will not have access to the stored images (with the exception of DHS and the Labs employees, and their subcontracted vendor partners as previously described). For example, the participating agency will only view the video images at the time the images are recorded and during subsequent project evaluation meetings and will only use those images to evaluate the technical capabilities and performance of the CICD system. Each of the demonstration attendees will be present in an official capacity, and access to the demonstration facilities will be controlled by authorized project personnel (DHS and the Labs) with appropriate physical security measures in place.

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

☐ Legislative authorization at the city or state level
☐ Executive or law enforcement decision
☐ Decision-making process included public comment or review
☐ Entity making the decision relied on:
- ☐ case studies
- ☒ research – S&T evaluated commercial systems and elected to proceed with the research because the existing systems do not meet end-user requirements.
- ☐ hearings
- ☐ recommendations from surveillance vendors
- ☐ information from other localities
- ☐ other (please specify)

Funding:
☐ DHS Grant
☐ General revenues
☐ Law enforcement budget
☒ Other (please specify) - DHS Science and Technology Program Funds
☒ Funding has limited duration (please specify) - CICD is a research program with limited duration, currently funded from the FY07, FY08, and FY09 DHS S&T Appropriations
☐ 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?

S&T, the Labs, and their subcontracted vendor partners will use the video collected during the CICD demonstrations for research and development purposes only. Demonstrations are intended to demonstrate the capability of the surveillance technology to local law enforcement and other federal agencies. S&T, the Labs, and the participating agencies will not attempt to use the equipment to identify any individuals. The video collected will be in a public setting and no attempts will be made to view private areas.

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 risk to the individual is that the individual's image could be collected and viewed by unauthorized personnel, and that law enforcement may base official law enforcement actions upon the research technology. To mitigate these risks, S&T and the Labs will control access to the images as they are collected and when they are stored. In addition, the participating agency will limit its involvement in this research project to providing feedback to S&T and the Labs regarding the capability and usability of the CICD technology. The agency will not engage in any routine law enforcement activity based on the images from CICD. S&T will post signage to notify individuals that the area is under surveillance. The purpose of collecting the images is to conduct research and development. S&T and the Labs will not use the images for any other purpose.

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.

S&T, the Labs, and their subcontracted vendor partners will use the images to evaluate system performance (digital image stitching for complex scenes, resolution, effectiveness of tracking tagged objects, change detection within a cluttered urban background), define system capabilities, consider the usefulness of the technology to end users, and make decisions on future program direction.

The CICD system and the images collected during the test will only be used for research and development purposes. However, in the event that a law enforcement investigation occurs due to an incident within the area monitored by the CICD system, the footage related to that specific incident could potentially be utilized during the course of the investigation.

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?

S&T will provide system training for authorized project personnel from S&T, the Labs, and their subcontracted vendor partners prior to the demonstrations. S&T will also brief individual observers from the participating agency prior to any interaction with the system. The training/briefings will include proper use of the system, a copy of this Privacy Impact Assessment, DHS privacy policies, and the protection requirements associated with the stored images.

Project image archives will be physically stored at the Labs. Access to the images will be granted by the appropriate Project Manager only after an authorized individual demonstrates a legitimate need for the images in order to conduct further research. While not in use, the images will be treated as sensitive information and be protected as such. This includes storing the archived images in a locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images. Each of the authorized individuals accessing the images will have completed training and/or briefings detailing DHS privacy policies including the protection of personally identifiable information.

Since testing of the CICD system represents a short-term research effort and not a permanently installed operational system that will generate records over the long term, no “system-specific”

auditing mechanisms are planned. The Labs, where the complete image archives will be physically stored, have IT security measures in place to ensure that the laboratory systems on which the images are stored are only accessed by authorized personnel. Should a privacy incident be suspected, the Labs would conduct an audit and immediately inform DHS.

Use of the stored images for research and development activities will be in accordance with the approved Statement of Work in the laboratory contracts with DHS.

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

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

There are no exemptions to the retention period.

The Labs will retain the images in order to allow review of system effectiveness in the demonstration phase and to make improvements in future phases of the project. The Labs and their subcontracted vendor partners will use the raw video images for research and development activities while adding additional capabilities to the existing demonstration system. The images will also provide a record of the system demonstration that may be reviewed by DHS program managers to characterize the effectiveness of the technology and recommend future program directions. The video images will be retained for the life of the project (of limited duration), and then be destroyed. Several years of research, development, and testing will be required to advance the technology to the point that an operationally-ready system can be produced. The project currently has funding anticipated in the Resource Allocation Plan through at least FY11, subject to availability of appropriations. Additional funding planned for surveillance research in FY12 –FY15 will likely be utilized at least in part to complete the project.

3.2 Retention Procedure

☐ Footage automatically deleted after the retention period expires
☒ System operator required to initiate deletion
☐ 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 Labs will retain the images in order to allow review of system effectiveness in the demonstration phase and to make improvements in future phases of the project. The Labs and their subcontracted vendor partners will use the raw video images for research and development activities while adding additional capabilities to the existing demonstration system. The images will also provide a record of the system demonstration that may be reviewed by DHS program managers to characterize the effectiveness of the technology and recommend future program directions.

S&T, the Labs, and their subcontracted vendor partners will make no effort to identify individuals and will not use the images for any purpose other than research and development.

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) –S&T program managers, S&T senior leadership, and potential customers (i.e., other DHS components such as the U.S. Secret Service). In all case, the images will be used and shared for research purposes and never to support operational activities.

☐ None

Classes of Personnel
☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☒ Other (please specify) – DHS program managers and subject matter experts

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)?

S&T will share the information with S&T program managers, S&T senior leadership and potential DHS Component customers for the purpose of program evaluation, defining system capabilities, considering the usefulness of the technology to end users, and making decisions on future program direction. (These individuals will not be given copies of the images—they will only be permitted to view a demonstration of system capabilities.) The raw images archives will be physically stored at the Labs. The Labs may provide limited images to S&T for the uses described above (i.e., review by DHS program managers and subject matter experts). S&T will appropriately safeguard all personally identifiable information in accordance with DHS privacy policies, to include storing demonstration images in a locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images.

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

☒ Yes (please detail)
☐ No

S&T has created the CICD Privacy Guidelines, which stipulates that users must have a legitimate "need to know" in order to have access to the images.

4.2.2 Is the grant of access specifically authorized by:

☒ Statute (please specify which statute) – Title 3 of the Homeland Security Act
☐ Regulation (please specify which regulation)
☒ Other (please describe) – The S&T Program Manager will authorize access to DHS program managers and subject matter experts for the purpose of program evaluation, defining system capabilities, considering the usefulness of the technology to end users, and making decisions on future program direction.
☐ 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)

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 research is that unauthorized personnel could gain access to the images collected during the experiment. To mitigate this risk, S&T will control access to the images and will grant access to DHS program managers and subject matter experts solely for the purpose of program evaluation, defining system capabilities, considering the usefulness of the technology to end users, and making decisions on future program direction. S&T will require any program manager or SME viewing the images to read this PIA to understand the privacy protection for the images.

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) – Local Law Enforcement Agencies
☐ State government agencies (please specify)
☒ Federal government agencies (please specify) – Pacific Northwest National Laboratory (Department of Energy); MIT Lincoln Laboratory (a Federally Funded Research and Development Center)
☐ Private entities:
- ☐ Businesses in monitored areas
- ☐ Insurance companies
- ☐ News outlets
- ☒ Other (please specify)

Selected images will be shared with research partners subcontracted to MIT Lincoln Laboratory and Pacific Northwest National Laboratory for research and development purposes.

☐ 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 footage

Participating Government Agencies – S&T will share the live-feed images with the participating agency in order to allow their personnel to evaluate the CICD system and provide feedback to the S&T program manager. The system requirements for CICD are largely based on prior discussions with these agencies defining their highest priority needs. Agency personnel will participate in the demonstration and will thereby have access to images feeds at the demonstration site. In addition, the agencies will receive a post-demonstration briefing to enable their senior management to evaluate the CICD system performance. For personnel participating in the CICD demonstration, a training that includes DHS privacy policies and instructions on proper use of the system will be required. Participants will be required to sign a copy of the CICD privacy guidance.

Pacific Northwest National Laboratory, MIT Lincoln Laboratory, and their subcontracted vendor partners – The images collected from the demonstration will only be used by authorized project personnel at Pacific Northwest National Laboratory, MIT Lincoln Laboratory, and their subcontracted vendor partners for research and development activities in accordance with the approved Statements of Work in the contracts with DHS and the Labs. For personnel participating in the CICD demonstration, a training that includes DHS privacy policies and instructions on proper use of the system will be required. Participants will be required to sign a copy of the CICD Privacy Guidelines.

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. The CICD system and the images collected during the test will only be used for research and development purposes. However, in the event that a law enforcement investigation occurs due to

an incident within the area monitored by the CICD system, the footage related to that specific incident could potentially be utilized during the course of the investigation.

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

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

If an MOU is not in place, explain steps taken to address this omission.

No MOU is currently in place between DHS and the participating agencies. However, participating agency personnel will receive a copy of this PIA and be required to participate in a training briefing.

The Labs are under contract to DHS to perform the tasks described in the CICD Statement of Work.

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

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, S&T will limit access to the stored images to authorized personnel at the Labs and their subcontracted vendor partners with a demonstrated "need to know." S&T will require all participants in the research, including lab personnel, their subcontracted vendor partners, and the participating agency, to read and sign the CICD Privacy Guidelines. By signing onto the guidelines, the Labs and their subcontracted vendor partners agree to protect the information by storing it in locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images.

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)

No one will be able to alter or enhance the images before or after storage. Only project research staff at the Labs will be able to delete the images.

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)
  Only personnel on-site for the CICD demonstrations (physically present with the CICD system) will have access to the real-time images. This includes personnel from the Labs, S&T, and the participating agency.
- ☐ All authorized users have access to stored data
- ☒ Only certain authorized users have access to stored data (please specify which users)
  Project research personnel at the Labs and their subcontracted vendor partners will store the images and will have access to it. S&T may have access to

limited sample images that could be used to demonstrate system capability to potential customers.

☐ All authorized users can control the camera functions (pan, tilt, zoom)
☒ Only certain authorized users can control the camera functions
The on-site demonstration personnel from the Labs, S&T, and the participating agency will control camera functions.
☐ All authorized users can delete or modify images
☒ Only certain authorized users can delete or modify images (please specify which users)
No one is authorized to modify the images. Only project research staff at the Labs may delete images.

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

☒ Yes (please specify)
S&T will require persons wishing access to the images to first demonstrate a need to know and to sign the CICD Privacy Guidelines before access to the images is granted.
☐ No

6.1.3 When access is granted:

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

The complete images archives will be physically stored at the Labs. Access to the images will be granted by the appropriate Project Manager at the respective laboratory only after an authorized individual demonstrates a legitimate need. While not in use, the images will be treated as "sensitive information" and be protected as such. This includes storing the archived images in a locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images.

Each of the authorized individuals accessing the images will first receive a copy of this PIA and undergo training and/or briefings detailing DHS privacy policies including the protection of personally identifiable information. Any sample images provided to DHS will be appropriately safeguarded as personally identifiable information in accordance with DHS privacy policies, to include storing demonstration images in a locked container or facility with access restricted to authorized individuals, and/or password protecting the electronically stored images.

6.1.4 Are there auditing mechanisms:

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

The CICD program is a research effort that will test a prototype system for a limited period of time. Since testing of the system represents a short-term research effort and not a permanently installed operational system that will generate records over the long term, no auditing mechanisms are planned. The Labs, where the complete images archives will be physically stored, do have IT security measures in place to ensure that the laboratory systems on which the images are stored are only accessed by authorized personnel.

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) – The training will consist of an oral briefing. All participants must sign a statement that they agree to the privacy guidelines at the conclusion of the briefing.

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

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)

As discussed in 6.1.4, the system represents a short-term research effort as opposed to a permanently installed operational system. No "system-specific" auditing mechanisms are planned. However, MIT Lincoln Laboratory and Pacific Northwest National Laboratory have IT security measures in place to ensure that images are safeguarded. Should a privacy incident be suspected, the Labs would conduct an audit and immediately inform DHS.

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 Labs and their subcontracted vendor partners will restrict access to the images to authorized individuals with a demonstrated need to know. The Labs and their subcontracted vendor partners will protect the images using physical and technical security measures. All personnel with access to the images will undergo training on the proper use and protection of personally identifiable information.

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
- ☒ Below is a copy of the wording of such notice signs
- ☐ Notice is not provided
- ☐ Other (please describe)

The Labs will post signs in the surveillance area stating: "This area is subject to video surveillance.

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

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 CICD demonstration is a research activity designed to evaluate the technology's performance. Since system resolution is a key component of CICD evaluation, the technology does not include mechanisms to blur or block images of persons and textual information captured in the public space. Should a DHS component or other federal government entity seek to acquire a permanent operational system, that entity would complete a PIA and evaluate the appropriateness of such design choices.

Responsible Official

John M. Fortune
Program Manager
Infrastructure/Geophysical Division
DHS Science and Technology

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security